The Challenges of Cloud Computing in Forensic Science

Raja Muhammad Ubaid Ullah[#1], Dr.Kevan A. Buckley[#2],Dr. Mary Garvey[#3], Dr. Jun Li[#4].
School of Mathematics and Computer Science
University of Wolverhampton, Wulfruna Street, Wolverhampton WV1 1LY, UK.

Abstract

Cloud computing (CC) is rapidly growing new information technology (IT) in private, public and especially in Government sectors internationally. CC technology facilitates rather than deploy and manage an in-house physical IT infrastructure by having local servers or personal devices to manage their softwares application. This new technology helps to transfer their traditional IT services model into remote, virtualised environments, which are often hosted and managed by the third parties. Therefore, CC environment of any organisation turn prospective opportunity for cyber attackers, which is become a primary challenges of CC in the protection of valuable data from different types of attacks. CC posed a serious risk and major challenge to digital investigators, also offers sufficient opportunities to investigators for better refining the forensic science. This study summarises the key areas of CC forensics science challenges and analyses by the researched performed by other researchers. The challenges also presented along with associated literature that particularly reference them. Finally the discussion and analysis, which is based on the study finding to consider the challenges provoke by the CC forensics science on our findings.

Keywords *- Cloud forensics, Digital forensics; Forensics; Cloud computing forensics; Forensic Science; Forensics challenges*

I. INTRODUCTION

CC is a new technology which is widely used by the different types of organisations to perform their day to day business activities in developed as well as developing Countries. The evolvement CC technology in the modern corporate market boosts competition to the utmost level, as result products and skills have become obsolete [1].But, there are some challenges are faced by organisations and businesses depending on their size and structure [3]. Organisations are also benefits by reducing operation costs and increasing their productivity by the adoption of CC services [1, 2]. Therefore, CC attracts as emergent modern technology in today's corporate sector, which provide the easiest availability of computational technology services for organizations through the internet.

The suitable use of Information and Communication Technologies (ICT) benefits businesses and organisation to become more proficient [1, 2, 4]. CC facilitates the organisations by providing resources and particular services by a user-pay system through the Internet [2, 3, 5]. CC technology generally offers a new corporate solution, which permits the organisations to rent the required information technology (IT) infrastructure, for instance, particular platforms, operating system, network hardware, storage, resources, the software through positioning their business applications and their data storage in the cloud environment [14]. There are many well-known cloud examples which include Amazon, Google and Microsoft (Department of Finance and Deregulation (DFD), [2, 6].

The worldwide public cloud services market is projected to grow 17.5 percent in 2019 to total $214.3 billion, up from $182.4 billion in 2018, according to Gartner, Inc.[9] The fastest-growing market segment will be cloud system infrastructure services, or infrastructure as a service (IaaS), which is forecast to grow 27.5 percent in 2019 to reach $38.9 billion, up from $30.5 billion in 2018 (see Table 1). The second-highest growth rate of 21.8 percent will be achieved by cloud application infrastructure services, or platform as a service (PaaS).

"Cloud services are definitely shaking up the industry," said Sid Nag, research vice president at Gartner. "At Gartner, we know of no vendor or service provider today whose business model offerings and revenue growth are not influenced by the increasing adoption of cloud-first strategies in organizations. What we see now is only the beginning, though. Through 2022, Gartner projects the market size and growth of the cloud services industry at nearly three time the growth of overall IT services."

Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	45.8	49.3	53.1	57.0	61.1
Cloud Application Infrastructure Services (PaaS)	15.6	19.0	23.0	27.5	31.8
Cloud Application Services (SaaS)	80.0	94.8	110.5	126.7	143.7
Cloud Management and Security Services	10.5	12.2	14.1	16.0	17.9
Cloud System Infrastructure Services (IaaS)	30.5	38.9	49.1	61.9	76.6
Total Market	**182.4**	**214.3**	**249.8**	**289.1**	**331.2**

BPaaS = business process as a service;
IaaS = infrastructure as a service;
PaaS = platform as a service;
SaaS = software as a service

With the increasing use of CC services in the organisations, there are always stays risk of data security and privacy, therefore the security concerned challenges are also increasing [10]. The digital source is an important aspect of digital forensic science which enforce to use different types of tools and techniques. CC is a greatly encouraged and enhanced way to store valuable data, as it diverts the researcher attention that research is being carried out for different types of challenges, opportunity and also to analyse and perform experiment over it. CC concept refers to provide different types of services to organisation remotely. Many organisations adopt the different types of CC services due to anytime and anywhere availability of data and also to utilise the required any type of application remotely [11].

In this type of situation where cloud forensic science is needed, but still cloud forensic science is not considerable developed theory. According to the author in [7, 8], there are many complexchallenges faced by investigator during the collection of require data also there are diverse types of issue on which investigator has to encounter to get the evidence of suspect.

The investigator has several problem, for instance, the storage of data is not local once kept on cloud, therefore suspects computer have nothing stored in the computer. This results that the data stored on cloud is of several user so the server cannot be seized unless all the user's data are seized.

If the suspect data is found, but still separating it from other users data is very complex exercise. As the data is on cloud environment the theft can be done, so it's a quiet high risk for the sensitive date like health related data, any type of national data and especially security related data. There are some different challenges, for instance, data acquisition, logging, chain of custody, limited forensic tools, trustworthy data retention, etc

Digital source is an important aspect of digital forensic science which enforce to use different types of tools and techniques. CC is a greatly encouraged and enhanced way to store valuable data, as it divert the researcher attention that research is being carried out for different types of challenges, opportunity and also to analyse and perform experiment over it. CC concept refers to provide different types of services to organisation remotely. Many organisations adopt the different types of CC services due to anytime and anywhere availability of data and also to utilise the required any type of application remotely [11].

CC is widely debated research topic but still, it presents numerous economic opportunities and encouraging technology [12]. The concept of IT is a setup of infrastructure for an organization with some boxes of hardware, applications, network switches, data canters, etc. whereas, the visualization of some computers connected with server and respective network for sharing different kinds of stuff, for instance, application, data with a low cost, maintenance free IT infrastructure which is called Cloud‖ [13, 14].

CC environment is a flexible elimination of resources, which includes multiple stakeholders and delivers a measured service at several layers for a specified level of service. CC Technology is switching traditional setup with virtualized, remote, on-demand software services, configured for the specific requirements of the organization.

These different types of required services can be hosted and managed by in-house or by any third-party. Which, resulting, the particular software and respective data comprising business application may be physically stored through different geographic locations. The use of CC services has prospective benefits to organizations, for instance, increased flexibility and efficiency. Apart from flexibility, efficiency and substantial cost saving, CC services offer a thread to the organization about a different kind of Copy Right theft or patented methods, solutions, or personal or organisational confidential information

II. WHAT IS CLOUD FORENSICS?

Computer forensics is an art and science of preserving, collecting,confirming, identifying, analysing, recording, andpresenting crime scene information. Wolfe defines computerforensics as "a methodical series of techniques and proceduresfor gathering evidence, from computing equipmentand various storage devices and digital media, that can bepresented in a court of law in a coherent and meaningfulformat" [15].

Forensic science is usually defined as the application of science to the law. Whereas, forensics, also known as computer and network forensics, generally has many definitions. Typically, it is reflectedin the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Data refers to well-defined pieces of digital information that have been organised in a precise way. Normally organizations have an increasing amount of data from different sources. For instance, data can be stored or transferred by standard computer systems, networking equipment, computing peripherals, personal digital assistants (PDA), consumer electronic devices, and various types of media, among other sources [16].

Definition according to the National Institute of Standards and Technology(NIST) [16],computer forensic is "an applied science to identify anincident, collection, examination, and analysis of evidencedata". There are also some other researchers define computerforensics as the procedure of examining the computer system todetermine potential legal evidence [17, 18].

III. CLOUD FORENSICS SCIENCE CHALLENGES.

According to (NIST), the major challenges of Cloud Forensics are categorised into the following nine major groups which are mentioned below: [31]

- ***Architecture*** (e.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc.).
- ***Data collection*** (e.g., data integrity, data recovery, data location, imaging, etc.).
- ***Analysis*** (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.).
- ***Anti-forensics*** (e.g., obfuscation, data hiding, malware, etc.).
- ***Incident first responders*** (e.g., trustworthiness of cloud providers, response time, reconstruction, etc.).
- ***Role management*** (e.g., data owners, identity management, users, access control, etc.).
- ***Legal*** (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.).
- ***Standards*** (e.g., standard operating procedures, interoperability, testing, validation, etc.).
- ***Lack of Training*** (e.g., forensic investigators, cloud providers, qualification, certification, etc.).

Cloud forensics applies this same forensic process but has the challenge of combining various physical and logical locations. These areas include the following [21]:

- **Client-side**. Technical controls or monitors implemented on networks and computers under client control or ownership (Intrusion Detection System [IDS], Web Content engine logging, firewalls, access log, chat logs [locally], etc.).
- **Combined-side**. Technical controls or monitors implemented on networks and computers allocated to cloud customers (access logs, transaction logs, usage logs, etc.).
- **Provider-side**. Technical controls or monitors implemented on networks and computers that support or comprise the cloud service (firewalls, load balancers, admin access logs, IDS, NetFlow data, etc.).

According to NIST and some other researcher describe the process for performing digital forensics comprises. Regardless of the situation, the forensic process comprises the following basic phases: [16, 19, 20, 21, 22]:

- **Collection.** The crucial and important phase in which to identify, label, record, and acquire data from all the relevant possible sources of related data, although following standard guidelines and procedures that help to preserve the integrity of the data. The process of collection is typically accomplished in a timely manner because of the possibility of losing effective data, for instance, current network connections, as well as losing data

from battery-powered devices (e.g., cell phones, PDAs).

- **Examination.** The examinations phase include forensically processing any volume of collected data using a combination of automated and manual methods to assess and then extract data of particular interest while preserving the integrity of the data.
- **Analysis.** The analysis phase is the process to analyse the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- **Reporting.**In reporting phase the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. Whereas, the formality of the reporting step varies greatly depending on the situation.

IV. FORENSIC STAFFING

Practically every organization needs to have some capability to perform computer and network forensics. Without such a capability, an organization will have difficulty determining what events have occurred within its systems and networks, such as exposures of protected, sensitive data. Although the extent of this need varies, the primary users of forensic tools and techniques within an organization usually can be divided into the following three groups [16]:

- **Investigators.** Investigators within an organization are most often from the Office of Inspector General (OIG), and they are responsible for investigating allegations of misconduct. For some organizations, the OIG immediately takes over the investigation of any event that is suspected to involve criminal activity. The OIG typically uses many forensic techniques and tools. Other investigators within an organization might include legal advisors and members of the human resources department. Law enforcement officials and others outside the organization that might perform criminal investigations are not considered part of an organizations internal group of investigators.
- **IT Professionals.** This group includes technical support staff and system, network, and security administrators. They use a small number of forensic techniques and tools specific to their area of expertise during their routine work (e.g., monitoring, troubleshooting, data recovery).
- **Incident Handlers.** This group responds to a variety of computer security incidents, such as unauthorized data access, inappropriate system usage, malicious code infections, and denial of service attacks. Incident handlers typically use a wide variety of forensic techniques and tools during their investigations.

Many organizations rely on a combination of their own staff and external parties to perform forensic tasks. For example, some organizations perform standard tasks themselves and use outside parties only when specialized assistance is needed. Even organizations that want to perform all forensic tasks themselves usually outsource the most demanding ones, such as sending physically damaged media to a data recovery firm for reconstruction, or having specially trained law enforcement personnel or consultants collect data from an unusual source (e.g., cell phone). Such tasks typically require the use of specialized software, equipment, facilities, and technical expertise that most organizations cannot justify the high expense of acquiring and maintaining. As described in Section 3.1.2, organizations should determine in advance which actions should be performed by law enforcement officials. Also, when expert testimony is needed for legal proceedings, organizations might seek external assistance.

When deciding which internal or external parties should handle each aspect of forensics, organizations should keep the following factors in mind [16]:

- **Cost.** There are many potential costs. Software, hardware, and equipment used to collect and examine data may carry significant costs (e.g., purchase price, software updates and upgrades, maintenance), and may also require additional physical security measures to safeguard them from tampering. Other significant expenses involve staff training and labour costs, which are particularly significant for dedicated forensic specialists. In general, forensic actions that are needed rarely might be more cost-effectively performed by an external party, whereas actions that are needed frequently might be more cost-effectively performed internally.
- **Response Time.** Personnel located on-site might be able to initiate computer forensic activity more quickly than could off-site personnel. For organizations with geographically dispersed physical locations, off-site outsourcers located near distant facilities might be able to respond more quickly than personnel located at the organisation's headquarters.

- **Data Sensitivity.** Because of data sensitivity and privacy concerns, some organizations might be reluctant to allow external parties to image hard drives and perform other actions that provide access to data. For example, a system that contains traces of an incident might also contain health care information, financial records, or other sensitive data; an organization might prefer to keep that system under its own control to safeguard the privacy of the data. On the other hand, if there is a privacy concern within the team, for example, if an incident is suspected to involve a member of the incident handling team, use of an independent third party to perform forensic actions would be preferable.

V. TOOLS FOR PERFORMING

Current forensic tools are based on traditional forensic approaches, including formal methods to acquire information and a structured method to analyse artifacts with the intention to recreate or validate some series of events or retrieve missing information. These forensic tools fall into two general categories [21]:

- **Static**. Static analysis forensic tools analyse stationary data, the contents of hard drives or NetFlow data, obtained through a formalized acquisition process.
- **Live**. Live forensic tools collect and analyse "live" system data, accommodating the order of volatility, performing memory analysis, and providing methods for encryption key recovery

VI. SUPPORTING FORENSICS IN THE INFORMATION SYSTEM LIFE CYCLE

Many incidents can be handled more efficiently and effectively if forensic considerations have been incorporated into the information system life cycle. Examples of such considerations are as follows [16]:

- Performing regular backups of systems and maintaining previous backups for a specific period of time.
- Enabling auditing on workstations, servers, and network devices.
- Forwarding audit records to secure centralized log servers.
- Configuring mission-critical applications to perform auditing, including recording all authentication attempts.
- Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets**.**
- Maintaining records (e.g., baselines) of network and system configurations.
- Establishing data retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed.

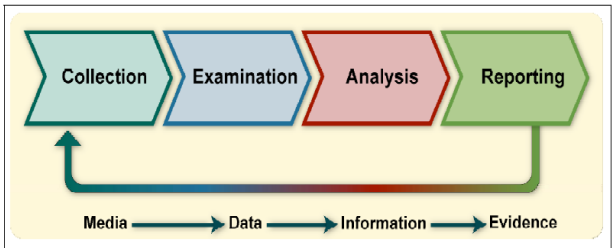

Fig 1: Forensics Process

VII. PRACTICE GUIDE FOR DIGITAL EVIDENCE

A. Association of Chief Police Officers (ACPO).

The document best practice guide has been formed by the ACPO Crime Business Area and was initially approved by ACPO Cabinet in December 2007. The main purpose of this document is to provide guidance not only to assist law enforcement but for all thatassists in investigating cyber security incidents and crime, originally approved by ACPO Cabinet in December 2007. [23].

B. The Principles of Digital Evidence [23]

- ***Principle 1:*** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- ***Principle 2:*** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- ***Principle 3:*** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- ***Principle 4:*** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

C. European Union Agency for Network and Information Security (ENISA)

The ENISA is basically a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. The main function of ENISA is to works with these groups to develop advice and recommendations on the good practice with respect to information security. It also assists EU member states with respect to implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks [24].

In cloud computing (CC) the threats to cybersecurity and cyber-attacks respect no organisational and their territorial boundaries. For this purpose, effective cooperation between the communities at all levels is essential to streamline the interchange of the information and knowledge required to reduce vulnerabilities and offer effective reactions to cyber incidents. Among others, these communities include, Computer Emergency Response Teams (CERTs) with respect to particular business sectors, which might be affected by large-scale incidents, other incident responders within a country serving other communities, national/governmental (n/g) CERTs, law enforcement agencies (LEAs) and internationally recognised research and development organisations [24].

D. Principles Of Electronic Evidence Gathering

The *Electronic evidence guide - A basic guide for police officers, prosecutors and judges [25]*, developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project [26]), for example, identifies five principles that establish a basis for all dealings with electronic evidence.

- ***Principle 1: Data Integrity:***The more important principle is to must maintained the integrity of digital evidence at all stages. "No action taken […] should change data which may subsequently be relied upon in court." [27].
- ***Principle 2: Audit Trail:***An audit trail (often referred to as chain of custody or chain of evidence) is the process of preserving the integrity of the digital evidence. "Documentation permeates all steps of investigative process but is particularly important in the digital evidence seizure step. It is necessary to record details of each piece of seized evidence to help to establish its authenticity and initiate the chain of custody."[28]. Indeed, an "audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result."[29].
- ***Principle 3: Specialist Support:***the need of specialist support to be requested as soon as possible when evidence gathering raises some specific (technical issues). The situation in every case vary, because there exist so many different types of systems and respective technical situations, so it is almost impossible for any digital forensics expert to have the specific expertise how to deal with all these sorts of electronic evidence. That is why it is very crucial to call in the right specialists – either from internal orexternal team, but need the right equipment ready for specialist to perform their tasks.
- ***Principle 4: Appropriate Training:*** Very important is the prerequisite proper training for the success of the search and seizure of electronic evidence. Appropriate and continuous training should be provided to all first responders team dealing with digital forensic, particularly when they are likely to deal specifically with 'live' computer and access original data.
- ***Principle 5: Legality:*** "The*person* in charge of the investigation has overall responsibility for ensuring that the law and these principles [the principles of digital evidence] are adhered to [30]".

Legal guidance for the practitioner varies depending on the jurisdiction in which they reside. Further, a distinction must be made between legislative documents and guidance and principles provided by relevant governing bodies within the forensic industry. Examples of such guidance documents include the above-mentioned *Electronic evidence guide - A basic guide for police officers, prosecutors and judges* developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project) and the UK *ACPO Good Practice Guide for Digital Evidence*.

VIII. FIRST RESPONDERS TOOLKIT

The first responder should have a complete toolkit, which permits them to arrive at the scene and collect all available valuable evidence, also ensuring its integrity for later investigation purpose. First responder toolkit should include but is not limited to the following [24]:

- **Cameras (photo and video)**: used to capture images of the scene and record the state of digital exhibits.
- **A digital clock**: to be put on the pictures taken, so the timestamps are visible as image, not just as meta data.

- **Cardboard boxes** or **secure evidence bags**: for collecting evidence for transportation to the laboratory.
- **Writing equipment**: prepared log forms to document steps taken. They should include a column for time/date, action taken, picture reference, person doing the proceedings, pens and pencils for recording contemporaneous notes at the scene.
- A **flow chart** on how to proceed in different cases, e.g. when the computer is running, when the computer is networked, etc.
- **Gloves**: to protect against contaminants present at the scene.
- **Evidence inventory logs, evidence tape, bags, stickers, labels, or tags**: crucial to ensure the integrity and continuity of the evidence found at the scene.
- **Antistatic bags and equipment** and **non-magnetic toolkit**: to allow for the safe collection of evidence, protecting its integrity.
- **A check list of possible relevant legal issues to consider and a list of relevant contacts for getting legal advice where appropriate**: this check list of relevant legal issues is not intended to help first respondents actually resolve those issues, but merely to ensure that they spot (all of) the relevant issues; the list of relevant contacts for getting legal advice is to help ensure that first respondents will contact someone with legal expertise in an effort to comply with the law.

If on-scene acquisition is required or if there is a high probability that such an acquisition will take place on site some additional equipment needs to be part of the toolkit, namely:

- **Forensic Laptop** to allow on-scene acquisition (see for more detail Sub-section 4.2).
- Forensic **write protection device** to protect evidential exhibits.
- Devices (e.g. Firewire) to get a memory dump. To intercept network traffic a **hub** (rather than a switch) may be necessary.
- All needed **cables** should be in the kit
- **Sanitised media** to store image of any digital exhibits.

A toolkit of first responders' should be influenced by different types of media, which may be present at a crime scene. Generally, such types of the toolkit should comprise of equipment capable of gathering digital evidence from any standard PC/laptop devices, mobile phones, tablet PCs, smart TVs, game consoles and all other types of modern devices comprising digital storage media. When dealing with mobile phones it should be essential to use Faraday bags (A 'Faraday bag' is a bag that acts as a Faraday shield. This way electronic equipment can be protected from for instance lightning strikes and electrostatic discharges) to prevent changes to the device.

IX. FIRST RESPONDER FORENSIC LAPTOP

The specifications of the first responder forensic laptop required the following description of the basic hardware and software. When purchasing a suitable laptop many keys issues need to be taken into consideration. More important it should contain a latest and fast processor combined with a quiet sufficient amount of RAM to allow fast processing of the case at hand. The other devices are several USB (3.0 at the time of writing) ports that will be needed to support the usage of various peripheral devices such as portable hard disk drives (alternatively a small USB hub with additional connectors works as well). A fast hard drive with large capacity or an SSD (Solid State Disk) must be included, to allow disk images to be stored locally (additional external USB hard drives might be useful as well).

Hardware Recommendations (at the time of writing of this document):

- Processor – Intel i7, i9 or AMD equivalen.t
- RAM – 8GB+.
- Motherboard.
- USB ports – 4 minimum and USB 3 if possible.
- Firewire port – for device compatibility and creating memory dumps for example from digital cameras with firewire.
- Large enough hard drive – Solid State Drive
- Spare disks.

Besides the hardware, the operating system that is running on the forensic laptop is very important. The operating system should be forensically sound and the first responder must be aware of how the system works.

X. CONCLUSION

This paper reviewed the research of different researchers based on the importance of CC and cloud forensics science in the cyberspace, their respective advantage, architecture and different cloud models. Also reviewed the particular conventional methodologies and guidelines proposed for performing different types of digital forensics, resulting so far insufficient in a cloud environment. If the predicted forecast by the different sectors related to CC is correct, as more businesses and organisations will be moving their valuable data to the cloud environment in the near future. In conjunction with a continued increase in cyber-crime, this transformation could result there will be a serious demand to conduct forensic science investigation in a particular environment. Presently such type of

investigations would be obstructed due to the lack of particular guidance regarding methodology and related software tools required to recover respective evidence in a forensically comprehensive manner. As this is a basic need for legal prospective with respect to clouds including data retention and to examine the privacy of laws.

The responsibility also goes to the digital forensics community to concentrate on establishing verifiable standard mechanisms to evaluate any frameworks, respective procedures and latest software tools to use in a CC environment. Governments also involve and try to ensure that proper arrangements to be made to preserve valuable data for the purpose of investigation across borders, otherwise it becomes challenging to choose appropriate court or any legal systems to represent the case. Whereas, keep in mind that tool which is available to support any particular forensic investigation cannot completely capable to perform the required forensic investigation in cloud forensic science. Therefore, appropriate implementation of global recognize standards helps to increase the capacity of forensic science investigation to enhance the required performance of the cloud.

REFERENCES

[1] Journal: A Survey Based Investigation for Cloud Computing Adoption Internationally. Authors Raja Muhammad Ubaid Ullah, Dr.Kevan A. Buckley,Dr. Mary Garvey andDr. Jun Li. International Journal of Computer Trends and Technology (IJCTT) - Volume 67 Issue 4 - April 2019. ISSN: 2231-2803 United Kingdom. http://www.ijcttjournal.org Page 106

[2] Journal: A Systematic Literature Review of Factors Affecting Cloud Computing Adoption Internationally. Authors Raja M. Ubaid Ullah, Dr.Kevan A. Buckley,Dr. Mary Garvey andDr. Jun Li. International Journal of Computer Trends and Technology (IJCTT) - Volume 67 Issue 3 - March 2019. ISSN: 2231-2803 United Kingdom. http://www.ijcttjournal.org Page 41

[3] Journal: Factors Analysis of the Adoption of Cloud Computing Adoption In England. Authors Raja Muhammad Ubaid Ullah, Dr.Kevan A. Buckley,Dr. Mary Garvey andDr. Jun Li. International Journal of Computer Trends and Technology (IJCTT) - Volume 67 Issue 6 - June 2019. ISSN: 2231-2803 United Kingdom. http://www.ijcttjournal.org Page 18-30

[4] Journal:Effects of Industry Type on ICT Adoption among Malaysian SMEs. Authors Khong Sin Tan ,Uchenna Cyril Eze, and Siong Choy Chong.

[5] Article: Factors That Influence Adoption of Cloud Computing: An Empirical Study of Australian SMEs. Authors Ishan Senarathna, Carla Wilkin, Matthew Warren, William Yeoh and Scott Salzman

[6] Paper: Cloud Computing Strategy Direction Paper. By the Department of Finance and Deregulation (DFD) Cloud Computing Strategic, by the Australian Government.

[7] Article: Challenges and Proposed Solutions for Cloud Forensic. Authors Puraj Desai, Mehul Solanki, AkshayGadhwal, Aalap Shah and Bhumika Patel. Puraj Desai et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 5, Issue 1(Part 2), January 2015, pp.37-42. https://pdfs.semanticscholar.org/4d43/19304cba36bd73695f9be7c33155dac5c0fc.pdf

[8] Article: Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Authors Shams Zawoad and Ragib Hasan. February 2013. https://www.researchgate.net/publication/235712413_Cloud_Forensics_A_Meta-Study_of_Challenges_Approaches_and_OpenProblems

[9] Press Release: Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019. Stamford, Conn., September 12, 2018. USA. To contact Katie Costello, Gartner,katie.costello@gartner.com,https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

[10] Journal: Design of digital forensic technique for cloud computing. Authors DeoyaniShirkhedkar and SulabhaPatil. International Journal of Advance Research in Computer Science and Management Studies. Volume 2, Issue 6, June 2014, India. Pg. 192-194. https://www.academia.edu/7655461/Design_of_digital_forensic_technique_for_cloud_computing

[11] Journal: Some Forensic & Security Issues of Cloud Computing. Authors Ashish Badiye, Neeti Kapoor and Pooja Shelke. Volume 3, Issue 10, October 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering. India. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.428.5521&rep=rep1&type=pdf

[12] Workshop: Technical Challenges of Forensic Investigations in Cloud Computing Environments. Author Dominik Birk January 12, 2011 https://pdfs.semanticscholar.org/c776/0c5d82142813add66abc52eac589767df1f8.pdf

[13] Journal:Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. Authors G. Grispos, T. Storer, and W.B. Glisson. International Journal of Digital Crime and Forensics, Volume 4, Issue 2, Pages 28-48, 8 October 2014. https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf

[14] Journal: Cloud Computing Adoption in Enterprise: Challenges and Benefits. , Authors Raja Muhammad Ubaid Ullah, Dr.Kevan A. Buckley,Dr. Mary Garvey and Dr. Jun Li. International Journal of Computer Trends and Technology (IJCTT) - Volume 67 Issue 6 - June 2019. ISSN: 2231-2803. Pages 93-104. United Kingdom https://www.ijcttjournal.org/2019/Volume-67%20Issue-6/IJCTT-V67I6P116.pdf

[15] Book: The Best Damm Cybercrime and Digital Forensics Book Period. Authors Wiles, Jack/Reyes and Anthony. ISBN: 9780080556086. Print ISBN: 9781597492287. Publisher: Elsevier Science & Technology. Publication Year: 2011.

[16] Publication: Guide To Integrating Forensic Techniques Into Incident Response. Authors Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang. Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology (NIST) Gaithersburg, MD 20899-8930 August 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[17] Article: "Computer forensics–an overview," By Frederick Gallegos, CISA, CDE, CGFM, Copyright 2005, Information Systems Audit and control Association. All Rights Reserved. www.isaca.org. https://my.infotex.com/wp-content/uploads/2012/03/computer_forensics_overview_isaca.pdf

[18] Paper: An explanation of computer forensics. Author Robbins, J. (2008). National Forensics Center, 774, 10-143.

[19] Journal: Challenges and Proposed Solutions for Cloud Forensic. Authors Puraj Desai, Mehul Solanki, AkshayGadhwal, Aalap Shah and Bhumika Patel. Puraj Desai et al Int. Journal of Engineering Research and Applications,ISSN : 2248-9622, Vol. 5, Issue 1(Part 2), January 2015, pp.37-42. https://pdfs.semanticscholar.org/4d43/19304cba36bd73695f9be7c33155dac5c0fc.pdf

[20] Article: Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Authors Shams Zawoad and Ragib Hasan. 26th February 2013, Article https://www.researchgate.net/publication/235712413_Cloud_Forensics_A_Meta-Study_of_Challenges_Approaches_and_OpenProblems

[21] Newsletter: Cyber Forensics in the Cloud. Authors Scott Zimmerman and Dominick. The Newsletter for Information Assurance Technology Professionals, Volume 14 Number 1 • Winter 2011. https://www.csiac.org/wp-content/uploads/2016/02/Vol14_No1.pdf

[22] Conference: Forensic Process as a Service (FPaaS) for Cloud Computing. Authors AmnaEleyan and DerarEleyan. 2015 European Intelligence and Security Informatics Conference. https://www.researchgate.net/publication/302603537_Forensic_Process_as_a_Service_FPaaS_for_Cloud_Computing

[23] Document: Association of Chief Police Officers (ACPO). Author DAC Janet Williams QPM. Force/Organisation Metropolitan Police Service, Version 5, ACPO © 2012. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[24] Document: The European Union Agency for Network and Information Security (ENISA). Authors Supervisor of the Study: ENISA, Authors of the Study: ENISA and Philip Anderson (Northumbria University, UK). © 2014, ISBN 978-92-9204-111-3 doi: 10.2824/068545. https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport

[25] CyberCrime@IPA, EU/COE Joint Project on Regional Cooperation against Cybercrime, Electronic evidence guide - A basic guide for police officers, prosecutors and judges,Version 1.0, Authors: Jones, N., George, E., Insa Mérida, F., Rasmussen, U., Völzow, V. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp

[26] CyberCrime@IPA, Electronic evidence guide - A basic guide for police officers, prosecutors and judges, Op. cit. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp

[27] ACPO, ACPO Good Practice Guide for Digital Evidence, Op. cit., http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

[28] Book: Digital Evidence and Computer Crime, 2nd Edition, Authors: Eoghan Casey, eBook ISBN: 9780080472508, Imprint: Academic Press, Published Date: 23rd February 2004. https://www.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-08-047250-8

[29] ACPO, ACPO Good Practice Guide for Digital Evidence, Op. cit., p. 6. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

[30] ACPO, ACPO Good Practice Guide for Digital Evidence, Op. cit., p. 6. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

[31] Report: NIST Cloud Computing Forensic Science Challenges. Draft NISTIR 8006, National Institute of Standards and Technology (NIST), Interagency or Internal Report 8006, 51 pages (June 2014). Comments on this publication may be submitted to: Michaela Iorga. https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf