A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics

Mohammed Khanafseh[1], Mohammad Qatawneh[2]
King Abdulla II School for Information and Technology
The University of Jordan Amman-Jordan

Wesam Almobaideen[3]
The University of Jordan Department of Computer Science
Rochester Institute of Technology Dubai, UAE

***Abstract*—Digital forensics is a class of forensic science interested with the use of digital information produced, stored and transmitted by various digital devices as source of evidence in investigations and legal proceedings. Digital forensics can be split up to several classes such as computer forensics, network forensics, mobile forensics, cloud computing forensics, and IoT forensics. In recent years, cloud computing has emerged as a popular computing model in various areas of human life. However, cloud computing systems lack support for computer forensic investigations. The main goal of digital forensics is to prove the presence of a particular document in a given digital device. This paper presents a comprehensive survey of various frameworks and solutions in all classes of digital forensics with a focus on cloud forensics. We start by discussing different forensics classes, their frameworks, limitations and solutions. Then we focus on the methodological aspect and existing challenges of cloud forensics. Moreover, the detailed comparison discusses drawbacks, differences and similarities of several suggested cloud computing frameworks providing future research directions.**

***Keywords*—Digital forensics; cloud forensics; investigation process; IoT forensics; examination stage; evidence**

I. Introduction

Digital forensics refers to the science, which deals with the crimes that happened on the level of digital devices. The main purpose of digital forensics is to detect, extract, and analyze evidence from digital media and prepare it for the prosecution, so that a case can be presented in court [1][2]. Using digital devices as a criminal tool has enhanced the criminal's ability to do different activities of criminals such as hiding facts, updating facts and users' document, or any other unethical activity. This type of crimes, i.e. "cybercrimes" is an extension of classical crimes. To deal with different crimes that happened on the level of digital devices, the investigators must implement consistent and precisely defined forensic procedures.

The Investigation process of any digital crime depends mainly on identifying and collecting evidence from the resources. The digital evidence refers to any critical information relevant to proof of the crime. This information, which can be used and accepted in court, stored and transmitted in digital form [3][4].

Moreover, the investigation process is highly depending on the device type and the environment used, which means that there is more than one branch under digital forensics because digital devices can be traditional computers, mobiles, network devices such routers, etc. Several challenges have been faced by digital forensics which hampers in finding out digital evidences such as technical, legal, and resource challenges. Consequently, the investigation process for one digital device may not be used for the other device so, it is difficult to find out a process which is compatible with all devices and environments.

This paper gives a comprehensive survey of different digital forensics branches which help the investigator to proceed in its investigation process. Moreover, the survey focuses on challenges, frameworks, and solutions of cloud forensics. The rest of this paper is organized as follows. Section 2 presents an introduction to digital forensics; Section 3 discusses the main branches of digital forensics, their frameworks, solutions and drawbacks. Finally, the article is concluded with the outcomes based on many comparisons between different branches of digital forensics and future work.

II. Digital Forensics

The digital forensic process is still in its infancy, but it is becoming increasingly invaluable for researchers, and many researchers have recently been working to propose specific models for digital forensics. The first proposed models for digital forensics include four main stages: Acquisition stage, Identification stage, Evaluation stage, and Admission stage. Since then, many models have been proposed to explain the steps taken to acquire, identify and analyze the evidence obtained from different digital devices. Digital forensics has become commonplace due to the increasing spread of technology and the high level of technological dependency since the 20Th century. In tradition forensics, the evidence is something tangible that could identify the criminal, such as blood, fingerprint, and hair, but these evidences cannot be found at digital forensics. In general, digital word refers to something related to computer technology such as files and data in digital form, based on that digital evidence refer to anything that can be extracted from digital devices. Based on the increasing number of digital devices, and the highly

dependent on these devices on daily activity for different persons, the number of digital crimes was increased.

The number of digital devices that require analysis is also increased, and the storage volume for each device is also increased. These devices and their storage space increase the complexity of digital forensics process.

A standard framework which proposed to guide the process of digital forensics is important to accelerate the process of investigation, and to overcome different problems that faces the process of investigation such as huge volume of storage space on digital devices [5],[6]. Several frameworks were defined over the time; each of new frameworks tries to integrate new technology and methods over the previous one. Most of the research in recent years was more concerned with employing new methods and technology to improve current frameworks from different aspects such as from efficiency and accuracy aspects; other current research was concerned to dealing with new problems.

A. Various Definitions of Digital Forensics

Various definitions of digital forensics have been proposed by many researchers, depending on legal, criminal or a process perspective. This section discusses some of these definitions. Some of the proposed definitions are as follows:

1) The researchers in [5] established one of the first definitions of DF. They define a Digital Forensics (DF) as a branch of forensics science involved with the use of scientific techniques towards the preservation, collection, validation, identification, analysis, interpretation, and presentation of digital evidence derived from digital sources for the purpose of facilitating the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned actions.

2) Another definition of digital forensics is suggested by [7], the author defines DF as a widely used term referring to identification, acquisition and preservation, digital evidence analysis from various digital devices, not just computers such as camera, smartphone, tablet, IOT device, network device, and other digital devices.

3) Other researchers, such as in [8] define a simple definition of digital forensics as science for identifying, preserving, recovering, analyzing and presenting facts and evidence relating to digital evidence on digital device storage media. This definition is a good and general definition because it is a simple definition that divides the process of forensics into four main areas from identification to the presentation.

4) Another simple definition has been proposed in [1], which defines a digital forensics as science for detecting, extracting and analyzing evidence from digital media, and is one of the critical requirements in cyberspace. And the author through his definition defines the main purpose of digital forensics through the definition is to prepare a report accepted in a court.

B. Digital Forensics Frameworks

Many researchers have developed a new process models and solutions to improve digital forensics. Digital forensics as science has made significant progress not only in the field of technology but also in methodology improvement. The process model is the methodology used through digital forensics to conduct a research framework with a number of phases that guide the investigation process. Generally speaking, there is no standard framework for the investigation process because the investigation process depends on the area of investigation and on a variety of cases, e.g., cyber attachment by IT specialists, civil cases in a corporation, or criminal cases, so different investigators will follow different ways of investigating their investigation process. The standard method used through conventional digital forensic processes, such as in [9] [10] [11], consists of defining the sequence of dependent stages necessary for the investigation process. The frameworks used during the investigation process can be classified based on a number of stages and sub-stages used. If the framework used contains a few stages, then this framework will not provide much guidance for the investigation process. A framework that contains many stages, and each stage has sub-stages, with its usage scenario being more limited, may prove more useful. Therefore, none of the proposed frameworks can have a general purpose and be used on any type of investigation, but the idea of any proposed framework should be as general as possible, which could be applied to as many cases as possible. To date, various frameworks have been proposed in the field of digital forensics. For a specific case, each of the proposed frameworks attempts to refine a particular methodology, for a particular case, different model have the same steps for the same case. Earliest research on digital forensics focused on defining the process of digital forensics [6].

Recently, the frameworks that proposed in digital forensic focused on a specific stage of digital forensics stages such as (identification, collection, preservation, and examination analysis stages), such as triage framework [12][13], which has been developed for time-sensitive applications. By applying digital forensics triage, the investigator could find the related evidence, which can accelerate the investigation process to lead to the criminal rather than waiting for the whole report from the police which could take several months or even years. Many frameworks were proposed on different areas of digital field, such as in digital forensics in general, computer forensics, mobile forensics, network forensics, IoT forensics, and cloud forensics. Each proposed framework has its own characteristics such as number of stages and strategy used for evidence collection based on the area of implementation.

Digital forensics framework can be defined as a structure to support a successful forensic investigation. This implies that the conclusion reached by one computer forensic expert should be the same as that of any other person who has conducted the same investigation [14]. Standardized digital forensics framework consists from each of the following stages [5].

1) Identification stage: This stage recognizes an incident from indicators and determines its type.

2) Preparation stage, which entails the preparation of tools, techniques, search warrants and monitoring authorizations and management support.

3) Approach strategy that develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.

4) Preservation stage: The preparation stage involves the isolation, securing and preservation of the state of physical and digital evidence.

5) Collection stage that entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.

6) Examination stage which involves an in-depth systematic search of evidence relating to the suspected crime.

7) Analysis stage which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.

8) Presentation stage which involves the summary and explanation of conclusions.

9) Returning evidence that ensures physical and digital property is returned to the proper owner.

Many frameworks have been proposed for investigation digital crimes, where each framework consists of a set of upper stages, and some others contain all standard stages of the digital forensics model. Table I shows different digital forensics frameworks proposed by many researchers.

Table I presents the most common stages of different forensics frameworks, problems solved by each framework and defines the degree of complexity of these frameworks based on the number of branches used. The conclusion that can be reached from Table I is that there are a set of issues that are not taken into account in the proposed frameworks such as confidentiality, security awareness, and accuracy of the investigation process in specific through evidence collection and examination steps. Based on the standard stages of any digital investigation process, the digital forensics frameworks can be categorized into the following three main types:

1) General Frameworks: Such frameworks proposed between 2000 and 2010 and focused on defining the phases of typical investigations [17]. Examples of this type of frameworks are shown in Table II [18][19][20][21].

Table II contains the frameworks which can be classified under the first type of digital forensics. The table contains information about each framework, such as the name of the framework, the main stages of each framework, and more, the table contains the sub-stage for each stage of the framework such as in the identification stage, some frameworks in this type of digital forensics frameworks contain just the stage of identification but in other frameworks, this stage was divided into more than sub-stage such as in Lee framework which divides it into classify sub-stage and compare sub-stage. Furthermore, this table provides a comment row which contains the main comments on the individual frameworks. The strengths and weaknesses of the framework and the complexity of the frameworks depend on the number of main stages and sub-stages in the frameworks proposed.

1) Frameworks concerned with a specific case, and focusing on a particular stage of digital forensics: Different frameworks of this type have been suggested such as frameworks which deal with certain categories of cases like forensic network, computer forensics, IOT forensics and other forensics, and frameworks that proposed for sensitive cases like abductions, missing person cases, etc., [22], [12]. At the early stages of digital forensics science, the proposed digital frameworks faced different issues, one of the urgent issues is to define the process model to make the entire investigation process consistent and standardized, general process model have been defined for investigation process, later framework that proposed contain additions stages for process model and with sub stages for main stages that forms the early framework, many of the new frameworks that have been proposed for digital forensic investigation which depends mainly on early suggested frameworks, Table III shows both original frameworks and updated frameworks, each of new proposed frameworks depends on the stages and strategy of investigation on conventional framework such as the SRDFIM framework which proposed in 2011 depends on the framework which called DFRWS framework, and many other frameworks as mentioned in Table III.

2) Frameworks have been proposed in recent years to deal with new technology such as cloud computing forensics, IOT forensics, etc. Some of the latest technology leads to new problems hampering digital forensic investigations, such as the problems that arise in cloud computing forensics. Cloud computing forensics faces many problems through each stage of the investigation process, such as the difficulty of identifying the right resources through the identification stage, matching the right evidence through examination and collection phases, etc. Other problems are caused by the use of digital forensics in the crime that occurred in the smart environment containing IoT devices, because more digital devices connected to the internet result in an ever- increasing volume of data. Based on these problems faced by forensics on new technology, a new integration between forensics processes and new technologies such as mining algorithms, security algorithms, data integrity and authentication algorithms that proposed to overcome all these problems, new frameworks were proposed in other more sophisticated cases to address the problem that can be solved through integration.

Table IV shows the main frameworks and solutions that were proposed for the IoT environment. The table contains the main stages of each framework, the main idea and goal of each framework, the name of the technology that the framework developed to serve, the encouragement point to develop the framework, the main idea for the proposed framework and what is the enhanced point in the framework and the name of the original framework on which the proposed framework depends if it is found.

TABLE. I. MAIN FRAMEWORKS PROPOSED FOR DIGITAL FORENSICS

Framework Names	Digital Forensic Branch Name	—	Individualization Stage	Initialization Stage	Identification Stage	Collection Stage	Authentication Stage	Preservation stage	Evidence Reduction stage	Documentation stage	Analysis Stage	Examination Stage	Presentation Stage	Reporting	Decision Stage	Review Stage	Plan Stage	Transportation Stage	Complexity Stage	Other Stages	Contribution And Comments
Generic Process Model for Network Forensics	Network Forensics	✗	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	H	Y	The proposed framework contains main stages of digital forensics with incorporating a new stage for detecting [15]
A Framework for a Digital Forensics Investigation	Digital Forensics	✓	✗	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	L	N	This framework is primarily designed to group many of the earlier phases of digital forensics into preparation and identification, which comprises stages of collection, preservation and matching for evidence [16]
Integrated Digital Forensic Process Model (2013)[17]	Digital Forensics	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	*L*	*N*	This process Model is a standardized model for the digital forensics method that helps the investigators follows a uniform approach in a digital forensic investigation based on different models.
An Examination of Digital Forensic Models	Digital Forensics	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	*M*	*N*	The objective of this framework is to explore the development of digital forensic process models and construct specific forensic methodologies.
The Enhanced Digital Investigation Process Model	Digital Forensics	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗	*M*	*N*	The proposed framework aims to redefine the digital forensic process and progress.

Carrier and Spafford FW (2004)	Digital Forensics	✓	χ	✓	✓	✓	✓	✓	χ	χ	✓	✓	χ	✓	✓	✓	χ	χ	*M*	*N*	In this framework the techniques of digital investigation are categorized on the basis of something beyond the previous experiences and subjective preferences of the investigator
Integrated Digital Forensic Process Model (2013)	Digital Forensics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	χ	χ	✓	χ	χ	*H*	*Y*	The main purpose of this framework is to propose a standardized model for digital forensics to help the investigators to follow a uniform approach in digital forensic research.
Data reduction and Data mining Framework for Digital Forensic Evidence (2013)	Digital Forensics	✓	χ	✓	✓	✓	✓	✓	✓	✓	✓	✓	χ	✓	✓	✓	✓	χ	*H*	*Y*	The goal of this framework is to reduce the volume of collected evidence to improve the review and investigation process.
Network Intrusion Forensic Analysis using Intrusion Detection System	Computer Forensics	χ	χ	χ	✓	✓	✓	χ	χ	χ	✓	χ	χ	✓	χ	χ	✓	✓	*H*	*N*	The author shows major challenges in computer forensics, intrusion detection system specialized model.
UML Modeling of Digital Forensics Process Models (DFPMs)	Digital Forensics	χ	χ	χ	✓	✓	✓	χ	χ	χ	χ	χ	χ	✓	χ	χ	χ	χ	*L*	*Y*	A lot of digital forensics process model has been successfully used in digital forensics, proposed model aimed to model some of the proposed process by using UML specifically the behavioral, use cases and activity diagrams.
Computer Forensics Investigation an Approach to Evidence in Cyberspace	Computer Forensics	χ	χ	χ	✓	✓	✓	χ	χ	χ	✓	χ	χ	✓	χ	χ	✓	✓	*H*	*Y*	This framework aims to define a new approach to solve and enhance the stage of computer forensics examination. The model meets Italian legislation and could probably be used in other countries as well.

Mapping Process of Digital Forensic Investigation Framework (2008)	Digital Forensics	χ	χ	χ	✓	✓	✓	✓	χ	χ	✓	χ	χ	✓	χ	χ	✓	✓	*M*	*Y*	The framework aims to produce the mapping process between activities and output from each phase of investigation framework, resulting in the creation of a new framework to optimize the entire Investigation process in digital forensics.
Common Process Model for Incident and Computer Forensics (2007)	Computer Forensics	χ	χ	χ	✓	✓	✓	χ	χ	χ	χ	χ	χ	χ	χ	χ	✓	χ	*L*	*N*	A new framework proposed for both Incident Response and Computer Forensics processes that combine their advantages in a flexible way: it allows for a management oriented approach in digital investigations while retaining the possibility of rigorous forensics investigation.
A Blockchain-based Process Provenance for Cloud Forensics (2017)	Cloud and Digital Forensics	χ	χ	χ	✓	✓	✓	✓	✓	χ	✓	✓	✓	✓	χ	χ	✓	χ	*M*	*Y*	The proposed framework uses blockchain technology in order to increase overall investigation efficiency and reliability.
An Integrated Lightweight Block chain Framework for Forensics Applications of Connected Vehicles (2018)	Internet of Vehicles and IOT Forensics	χ	χ	χ	✓	✓	χ	✓	✓	✓	✓	✓	χ	χ	χ	χ	χ	χ	*L*	*N*	The proposed framework uses block chain technology in order to improve safety and integrity of the collection stage.
Block chain based digital forensics (2017)	Digital Forensics	χ	χ	χ	✓	✓	χ	✓	✓	χ	✓	✓	✓	✓	χ	χ	χ	χ	*L*	*Y*	The proposed framework uses block chain technology in order to achieve integrity, authenticity, security and auditability for investigation process.

TABLE. II. MAIN STAGES FOR THE FRAMEWORK WHICH PROPOSED IN EARLY DAYS OF DIGITAL FORENSICS

Framework Name	Stage One and it's sub-stages	Stage two and it's sub-stages	Stage three and it's sub-stages	Stage Four and it's sub-stages	Stage five and it's sub-stages	Stage Six and it's sub-stages	Comments
Lee FW (2001)	Recognize (Document and collect and preserve)	Incident recognition	Identify Sub-stage Classify Sub-stage Compare Sub stage	Individualize stage Evaluate sub-stage Interpret sub-stage	Reconstruction Stage Reporting Sub-stage Presentation Sub-stage		The proposed framework has three stages: identification, individualization and reduction. This framework can be considered as a framework of medium complexity as there are not many phases.
Casey FW (2004)	Incident recognition	Assessment Stage	Resource identification and seizer stage	Preservation Stage	Examination Stage Recovery harvesting Reduction classification	Analysis sub-stage Reporting sub-stage	The proposed framework contains all stages of the conventional framework with an addition to new stages such as assessment, incident recognition stages. This framework can be classified as a highly complex framework based on the addition of new stages to the standard stage and on numerous sub-stages in the examination stage.
Cohen FW (2009)	Identification Stage	Collection Stage	Transportation Stage	Storage Stage	Examination Stage Analysis Interpretation Attribution Reconstruction	Presentation Sub-Stage Destruction Sub-Stage	Proposed framework contains all stages of standard framework with addition of some stages such as the storage stage in place of preservation stage and the stage of destruction which added as a new stage to make sure that all collected evidence was deleted from the investigator side. Proposed frame work can be classified as a medium complexity and efficient framework.
Baryamureeba and Tushabe FW	Readiness Stage operational Readiness sub-stage Infrastructure readiness sub-stage	Deployment Stage Detection and notification Sub-Stage Investigation conformation submission	Trace back Stage Digital crime scene investigation sub-stage Authorization Sub-Stage	Dynamite Stage Physical crime scene investigation Sub-Stage Digital crime scene investigation Sub-Stage Reconstruction Sub-Stage Communication Sub-Stage	Review Stage		Proposed framework contain stages completely different from the stages of conventional frameworks, such as the readiness stage which refers to the preparation and pre-investigation stages, this stage contains a lot of sub-stages which add a thing of complexity to the framework. This framework can be classified as a highly complex framework because it contains a lot of new stages and sub-stages, for each of these stages.

TABLE. III. NEW FRAMEWORKS FOR DIGITAL FORENSICS DEPENDING ON EARLY FRAMEWORKS

Traditional framework	Novel frameworks
The proposed framework DFRWS 2001[5] consists of four main stages, preparation stage, identification stage, authorization and communication stage.	The proposed SRDFIM framework, 2011[23], consisting of set of stages, preparation stage, scene securing stage, screening stage recognition, scene documentation, communication shielding, evidence collection, preservation, screening, analysis and presentation stage.
IDIP framework 2003 [24], this framework consists of a set of phases starting from the crime scene preservation phase, Crime Scene Survey, Crime Scene Documentation, Crime Scene Search, Crime Scene Reconstruction.	The proposed CFFTPM 2006 framework [13] depends primarily on the IDIP framework and the CFFTPM framework consists of two main stages, the preparation stage and the analysis stage. The preparation stage consists of a set of sub-stages such as preparation, collection, and preservation of identification, and the second main stage is the analysis stage containing sub-phases such as examination, analysis and presentation.
An Integrated Digital Forensic Process Model 2013 [6] consisting of stages such as documentation stage, preparation stage, incident stage.	DFaaS Framework 2014 [25], phases of the DFaas Framework are dependent on the main stages of the IDFPM framework, starting from digital evidence collection and authentication, collection phase in this framework is different from the original framework because the evidence collected will be stored in central storage. After that the next stage in the proposed framework is the examination phase that was carried out using the current examination tools, then the results of the tools used through the examination phase are stored in the centralized database, then the reduction and analysis for the extracted information and then the presentation phase.

TABLE. IV. MAIN DIGITAL FORENSICS FRAMEWORK FOR DIFFERENT FIELDS OF TECHNOLOGY

Framework Name	Martini Framework 2012 [26]	Quick and Choo Framework 2014[27]	Perumal Framework 2015[28]
Main Stages	Evidence Source Identification. Evidence Collection. Evidence Preservation. Examination Information. Analysis Stage. Reporting Stage. Presentation Stage.	Commence. Preparation. Identify and Collection. Reduction by Reduce Data Collection. Review and Data Mining. Open and Close Source Data. Evidence analysis. Presentation. Complete	Plan. Evidence Identification. Examination. Analysis. Archive and Storage.
Technology name which can use the given framework	Cloud Computing, proposed frameworks specialized to solve the problem of investigation in cloud level.	For any digital forensics process that deals with a huge volume of information	Internet of Things specialized for IOT investigation process.
Main encouraged points	Huge volume of data, transferring evidence from remote location. Volatile data. No possibility to physically seizing all the servers in a cloud computing environment.	Slow analysis and examination process based on huge volume of information gather through collection stage	The increasing number of IoT devices connected will increase the quantity of evidence required by any investigative process.
The Idea from proposed Framework	Overcome set of issues that faces previous frameworks when applied in cloud computing environment such as volatile data gathering, collection of metadata that can help on investigation process	Reducing the amount of collected information by acquiring a subset of the data by utilizing data reduction and conduct intelligence analysis through data mining	Define a standard operating procedure for investigation of IOT de vices
The original framework on which the framework proposed is based	McKemmish 1999[9] and Kent et al. 2006 [10].	McKemmish's (1999) [9] framework with the intelligence analysis cycle.	Triage model and 1-2-3 zone model for volatile based data preservation [12].

C. Main Challenges in Digital Forensics Process

According to research papers [29] [30], and [28], the main challenges of digital forensics can be classified into categories as listed below:

1) The diversity problem: Due to the fact that the digital forensics primarily depend on evidence collected from several digital device types, like computers, tablets, servers, camera and others, each of these devices has its own data format and can pose an important challenge during the analysis phase, because the evidence gathered is not standardized.

2) The efficiency of current digital forensics tools: Many of the digital forensic tools developed have been intended for finding at least one part of evidence, but they can be useful in other applications including standardizing different formats, compressing the collected evidence, extracting critical information and other tasks.

3) The volume of data collected from digital devices is huge, because of the growing number of digital devices used in our lives today. This huge volume of information causes difficulties at various stages of the digital forensic research process, such as the problem through the phase of evidence analysis, examination phase and other problems.

4) The complexity of format: This problem arises from data format collected from various digital devices requiring complex data reduction and review techniques.

5) The unified time lining issue: Based on gathering evidence from multiple digital devices, where multiple sources present different time zone references, timestamp interpretations, clock skew/drift issues, and the syntax aspects involved in generating a unified timeline.

6) Lack of training and resources: Any researchers manually inspect the need for a specific tool to utilize through the investigation process, and for this lack of training and resources, which refers to one of the major challenges faced by the digital forensic, specific training is required for these tools.

D. The Importance of Digital Forensics

In recent years, digital forensics has become important as the computer and cellular markets have grown. Based on the increased demand on smartphones, computers, and digital dependent through daily process, the market for malware or spyware has increased, digital forensics encompasses a variety of duties, such as the ability to recover different digital data, recover deleted data such as deleted messages from smartphones, deleted log files for different browsers, analyze and extract information and detect and remove different digital malware's or spy-wares. Malware or spyware refers to a program that allows for attackers to spy on user activities. Both malware and spyware are considered as a cyber-crime that can be extremely detrimental to you as an individual [31].

Adding the ability to applied digital forensics in computer resources will help in ensuring that the overall integrity and survivability of your network infrastructure, other implementing computer forensics can help the organization if you consider that computer forensic as a new basic element in what is known as a defense-in-depth (Defense in depth is designed on the principle that multiple layers of different types of protection from different vendors provide substantially better protection) approach to computer security and network security. Other important point of digital forensics is that DF can track where the user was or things started wrong before deleting it, while others can track down hackers even if the most important part of a digital hard drive is destroyed. When digital forensics are ignored or miss practice, essential evidence inadmissible legal evidence is entreated or collected. Others may escape new legislation mandating regularity compliance. The correct application of the forensics models may contribute to the prosecution of offenders. Digital forensics can provide feedback on improving current mechanisms for prevention to prevent a repetition of the event.

III. Main Branches of Digital Forensics

Digital forensics is used to investigate crimes, where a digital device is used either as a tool in enabling the crime or as a target of the crime. As illustrated in Fig. 1 the digital forensics consists of a set of branches. Many process models have been proposed for each of these branches, through the following section we will go deeply into most of these branches and focus on the cloud forensics branch.

The main branches of digital forensics are shown in Table V, with detailed information about each branch. Moreover, Table V shows the differences between the five branches of digital forensics depending on a set of criteria such as goal, type of collected information, Coverage digital devices, and main stages.

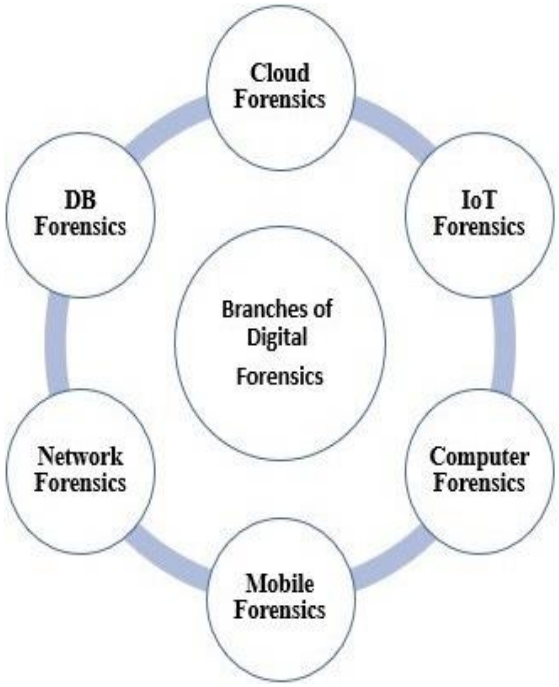

Fig. 1. Main Branches of Digital Forensics.

TABLE. V. COMPARISON BETWEEN MAIN TYPES OF DIGITAL FORENSICS BASED ON SPECIFIC PARAMETERS

Digital forensics branch name	Main Goals for DF Branch	Source of Evidence and type of information collected	Coverage digital devices	Main Stages of branch framework
Computer Forensics	The goal of computer forensics is to analysis information contained within and created with digital artifact; such as computer systems and electronic document.	Broad range of information start from log files such as inter net history, actual files stored in storage de vices, and static memory such as USB.	Traditional computers such as desktops, laptops, servers, tablets, etc.	Acquisition stage. Examination stage. Analysis stage Reporting Stage. Presentation Stage
Mobile Forensics	Recover digital evidence from a mobile device such as cellular phones, smartphones and mp3 players.	Communication information (SMS/ Emails), recovery of deleted data, contact numbers, photos in smartphones, notes, and other personal information	Mobile devices such as smartphones and mp3 players	Seizure stage. Acquisition stage. Examination and analysis stage.
Network Forensics	Monitoring, extracting and analysis of traffic on wired and wireless networks.	Routing tables, web browser history log, router logs, website pages, email attachments, VOIP data	Routers, internet applications, VOIP telephone, etc.	Identification stage. Preservation stage. Collection stage. Examination stage. Analysis stage. Presentation Stage.
DB Forensics	Study and analysis of databases and their metadata for incidents such as security attacks.	Database content, Metadata information, cached information which may locate in server RAM, database transactions, and queries.	Storage center, cash memory, servers RAM.	Identification Stage. Collection stage. Analysis Stage. Documentation Stage. And Presentation Stage [33].
IOT Forensics	Recovery of digital evidence form IoT devices such as sensors.	IOT applications, Smart home applications, sensor logs and information, and CSP log files	IOT devices such as sensor nodes, cars, smart applications.	Collection Stage. Examination Stage. Analysis Stage. Presentation Stage.
Cloud Forensics	Investigate the crimes that have occurred in cloud computing environments because it has many weaknesses, such as the nature of cloud computing, which can help to increase the level of crime	Users devices connected to the cloud computing environment, servers and storage center of cloud computing, cloud service provider	Laptops, desktops, smart phones, storage center devices and tablets	Preparation stage Identification stage Evidence collection Examination and analysis Presentation and Reporting

- Computer Forensics

Computer forensics can be defined as a discipline that combines legal and computer science elements to implement various stages of digital forensics on computer resources to explain the state of a digital artifact such as computer systems and electronic document [33]. The goal of computer forensics is to analysis of information contained within and created with digital artifact; such as computer systems and electronic document. Digital information required for the investigation process must be derived from a digital source in a timely manner, and critical information needed for the investigation process must be derived in a short time period [22].

- Mobile Forensics

Mobile forensics Recovers digital evidence from a mobile device such as cellular phones, smartphones and mp3 players. In recent years, mobile devices have been the booming technological trends along with Internet of Things, Cloud Computing and Big Data. Smartphones offer a range of features, allowing users to perform nearly every task done on computers. Fig. 2 history of the distribution of mobile devices (smartphones, tableting) compared to desktop computers can be found in the following graph. Smartphone replaces computers in almost every way since the majority of applications, from private use to business, from photos to online banking, are portable and more convenient to use. This means that for many investigations' smartphones have valuable information. They give recent chats, call logs, location data, photos, etc., to help the forensic investigator identify the person and learn about their recent work. They carry more personal data than a traditional PC in most cases.

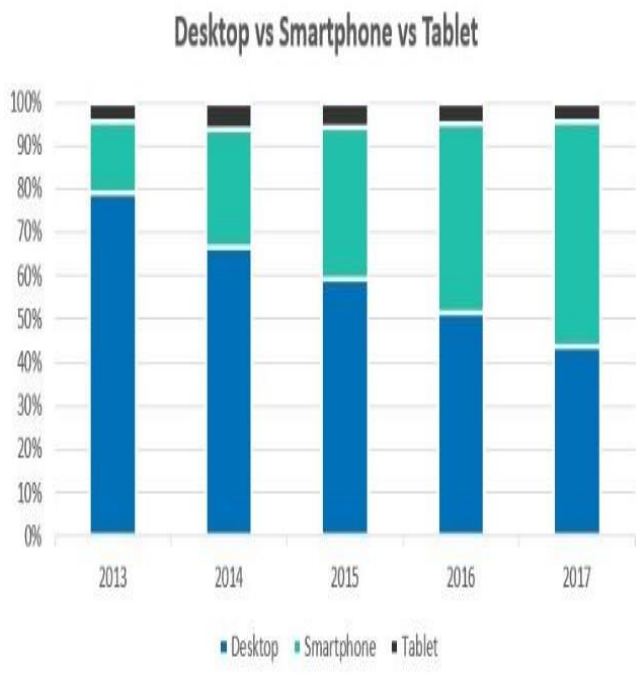

Fig. 2. History of the Distribution of Mobile Devices (SmartPhones, Tableting) Compared to Desktop Computers.

Many mobile forensic frameworks have been proposed, such as the framework proposed by Elhadje [34], the author motivated by the lack of mobile forensic frameworks to analyze and map data collected from various sources, including calls, geographical locations, multimedia, the proposed framework and others could contribute to a novel and potentially market-leading forensic mobile framework. Another framework proposed by M.Petraityte on the field of mobile forensics [35], the main objective of the proposed framework is to assist forensic investigators by potentially shortening the time spent investigating possible infringement scenarios. And many other frameworks and tools proposed with some update based on the nature of mobile devices in the field of mobile forensics with the same stages of digital forensics.

- Network Forensics

Network forensics is an extension of digital forensics, which can be defined as a network traffic investigation process that provides a means of monitoring various cyber-crimes by analyzing and tracking the evidence gathered from the network, and highlights the detection and prevention of different network attacks. Network forensics analysis tools can provide many functions such as network forensics and security investigation, data integrity from multiple sources, prediction of future targets for attacks, network traffic analysis, and recording various types of traffic analysis based on user needs, and many other functions can be provided by network forensics tools. The network forensics process can be applied on different network layers as follows [36][37]:

- Network forensics on Ethernet layer: The network forensics process can be applied on the Ethernet layer by eavesdropping bit streams with tools, called sniffing tools or monitoring tools. Famous tool for doing this is Wire-shark and d tcpdump, where tcpdump works primarily on Unix operating systems, which can assist the investigator in gathering various evidence on the Ethernet layer.
- Network forensics on network layer: Through network layer the internet protocol (IP) is responsible for delivery of packets generated by TCP through the network by adding both source address and destination address. The packets that sent from source node to destination node must go through set of routers, each router contains a routing table. The Routing tables are one of the sources for evidence in network forensics process, because it can help to track down the attackers by reverse the sending route and find the computer the packet came from. Other evidence resources in network forensics refer to network device logs that record traffic information. To reconstruct the attack scenario, multiple logs recorded from different network device can be correlated together. Network devices have limited storage capacity and network administrator can configure the devices to send logs to a server and store them for a period of time. The Network forensics have received a great importance due to the following facts:

1) Due to a large number of attacks through the network, like the DDOS attack on the social network and push attacks, different organization is mainly concerned about their network and data transfers through the network locally or publicly. For this, it is necessary to trace out the criminals, and collecting legal evidences is required through the trace operation to present them in the court. Based on this it is necessary to have forensics principles for network environment to collect evidence that can be used in the court of law.

2) For any investigation process it is necessary to use network forensics to analyze the historical network data in order to investigate security attacks by reconstructing sequence of security attacks.

3) Network forensics can do other than investigation on crimes happened on the network level. Network forensics can be used to address network issues of business-critical systems.

4) Network forensics is important to get trustworthy of users, and the ability to safeguard their interest. Network forensics can provide monitor and analyze their network traffic to detect malicious events and take actions for attack as quick as possible.

The network forensics branch faces a set of challenges such as data and traffic-related challenges. The graph below shows the main challenges faced by the network forensics, and proposed solutions [38]. The challenges faced by the forensic network have been identified in Fig. 3. various frameworks and solutions have been proposed in the field of network forensics, these solutions can be classified as follow:

- Distributed Network Frameworks and Solutions. A lot of frameworks and solution proposed in network forensics can fall under this type of network forensics such as the framework proposed by Shanmugasundaram et al. through [39], the author proposed a distributed network logging mechanism over wide area networks. [U+0650] Another distributed frameworks have been proposed through [40], [41]. And The framework of Mandia and Procise [42], which adding the two-way incident response stage between detection and presentation stages.
- Dynamic Network forensics frameworks, which used in large scale environment and depends on storing collected evidence in distributed DB to achieve level of security various frameworks fall under this category of network forensics frameworks such as the framework proposed in 2007 by Wang et al [43]. which proposed the model based on the artificial resistance theory and multi agent theory and the model proposed through [15], Kohn Framework [6], follows standard steps in digital forensics investigation processes, And the framework proposed by Liu in [44], which depends on using a logic-based network forensic process model using PROLOG to analyze the evidence collected and delete all unrelated data,
- Soft computing-based network forensic frameworks. Specified for an unsecured environment and environment that contains many attacks because this category of frameworks deals with the analysis of data collected and the classification of related attacks. This category of network forensics frameworks involves various frameworks such as [45], [46], and [47].
- Graphic Based Network Forensics Frameworks. Various framework were fall under this category such as the framework which proposed in 2008, Wang and Daniels. Proposed framework is graph-based approach for network forensics analysis [40] and [48].

- Internet of Things (IOT) Forensics v Internet of Things can be viewed as an information system made up of things, networks, data, and services. Such things may be wireless sensors, traditional computers, cameras, home appliances, tablets, smartphones, vehicles, humans, etc. that are connected over a network which can be wired or wireless. These things may gather, process, and upload a huge amount of data to the internet and used to initiate service. The architecture of IoT combines different zones such as perception zone, fog zone and cloud zone, where each zone can be a source of evidence in IoT forensics, such as evidence that can be selected from smart IoT devices, sensor nodes, firewalls, routers, etc. IoT forensics depends mainly on the main stages of digital forensics investigation such as the collection, examination, analysis and presentation of digital evidence with difference in some points such as source of evidence. IoT forensics could handle any possible format of data evidence, in traditional forensics it should handle electronic documents or standard format [49] [50]. IoT forensics process faces many challenges such as data location as many of the IOT devices are distributed in various locations that are out of user control, which can affect the investigation process. Moreover, IoT forensics process faces another challenges such as the limitation of the lifespan of digital media and the limitation of storage devices [51]. Table VI appears the famous proposed IoT forensics frameworks.

Fig. 3. Challenges Face network Forensics and Proposed Solutions for each Challenge.

TABLE. VI. MAIN FRAMEWORKS AND SOLUTION THAT PROPOSED IN IOT BRANCH OF DIGITAL FORENSICS

Framework Name	Initialization Stage	Identification Stage	Evidence Collection Stage	Reduction Stage	Preservation Stage	Examination Stage	Analysis Stage	Sharing With Another Investigators	Review Stage	Documentation Stage	Presentation Stage	Reporting Stage	Complexity Level	Comments And Limitation	Main Contribution
Generic Digital Forensics For IOT [52]	✓	✓	✓	χ	✓	✓	✓	✓	χ	χ	✓	✓	(*H*)	The proposed framework contains the basic stages of the digital forensics process, but it does not contain any strategy for feedback and evaluation, and the proposed framework does not concern privacy and integrity.	The forensics framework has been suggested as there is no framework available for investigating digital crimes that can occur in a smart environment. The importance of the proposed framework stems from the various safety principles proposed by the ISO standard
IoT forensics framework for smart environment [53]	✓	✓	✓	χ	✓	✓	✓	χ	χ	χ	✓	χ	(L)	The proposed framework is a privacy conscious framework that takes into account a set of privacy principles that can improve data privacy but, at the same time, is not suitable enough for IoT devices with limited resources.	The main goal for the proposed framework is to introduce a new lightweight version of the IoT forensics framework, that can be applied to investigate crimes that have occurred in the IoT environment to be suitable for the nature of the IoT devices.
Privacy aware IoT forensics process model [54]	✓	✓	✓	χ	✓	✓	✓	✓	✓	✓	✓	✓	(H)	The proposed framework is a privacy conscious framework that takes into account a set of privacy principles that can improve data privacy but, at the same time, is not suitable enough for IoT devices with limited resources.	Through this research paper, novel privacy conscious IoT forensics process model was proposed. The idea here is to achieve different principles proposed by ISO / IEC 29100:2011. The proposed framework consists of all basic stages of any forensic process model with the addition of new stages such as review stage, initialization stage, and feedback stage

IoT-Forensics Meets Privacy Towards Cooperative Digital Investigations [55]	✓	✓	✓	χ	✓	✓	✓	✓	χ	✓	✓	χ	(H)	The author has suggested an improved Model for an IoT environment investigation process that takes into consideration many of the concepts of privacy and security.	The idea from proposed model is to present a digital witness approach with methodology that enable citizen to share its sensitive information with investigators based on using PROFIT methodology.
Application Specific Digital Forensics Investigative Model in IoT [56]	χ	✓	✓	χ	✓	✓	✓	χ	χ	✓	✓	✓	(L)	The proposed model consists of basic stages of the forensic process, It does not take into consideration any principles such as privacy, integrity, and other security principles. .	The idea from this research paper is to introduce an application for a specific digital forensic investigation model, which will be applicable with any IoT related forensics investigation. Artifact of forensic importance in three highly adopted IoT applications scenario, smart home, smart city and wearable.

- Cloud Computing Forensics

Cloud computing can be defined as an internet-based computing paradigm in which a huge number of computer system resources such as computing power and storage are networked to enable users to remotely access and use these resources via the internet. Cloud computing can be categorized according to service model into three major types:

1) Infrastructure as a Service (IaaS) which delivers basic computer infrastructure as a service such as network capability and storage space.

2) Platform as a Service (PaaS) which refers to delivery of an entire computing platform and solution stack as a service.

3) Software as a Service (SaaS) which refers to provide a software which hosted centrally and can be accessed by any user using thin client, this not need to purchase and install.

A cloud forensics can be defined as a mixture of traditional computer forensics, digital forensics, and network forensics [57][58], other definition for cloud computing forensics was defined by [59] which define it as an application of digital forensics in cloud computing environments.

Other researchers, such as in [60], define cloud forensics as a part of network forensics that uses a fresh cloud-friendly technique to follow the primary stages of network forensics.

The suggested cloud forensics frameworks in [57] [59] show a set significance points of cloud forensic, these points and their evaluation results are as follows:

1) Cloud forensics is important component for cloud security.

2) There will be a lack of awareness until a major critical incident happens.

3) Cloud forensics is important to get the trust of the users who need to use cloud resources.

4) Cloud forensics needs more funding and investment in the RD than it has got at the moment.

The cloud forensics faces many challenges, here we exam ine set of challenges in cloud computing forensics as follows:

1) Unification of logs format: The cloud computing consists of a huge number of servers, where each server in cloud environment has its log format and this will hamper the investigation process as the evidence gathered will be in more than one format, this point makes the investigation more complex. Synchronization and time stamp, because of a large number of server's participants in a cloud system and the distributed locations for these servers, each of locations have a specific time zone. This can cause a problem through the investigation process in a cloud environment. One of solutions that suggested to solve the time zone problem is suggested by [61], which suggest a specific time system to be used on all entities of the cloud. This can achieve benefit of having a logical time pattern.

2) Missing terms and conditions in service level agreement (SLA) regarding investigations, where service level agreement is the main points and conditions between the user and the cloud service provider. These points should include important terms regarding cloud forensics investigation. Ruan et a1. [60] SLA should include: service provided, technique supported, access granted by CSP to the customer, security issue in multi-jurisdictional environment in terms of legal regulation, privacy policy and customer data.

3) Lack of forensics expertise, especially on the level of cloud computing.

4) Decrease access to forensic data and control over forensics data at all level from customer side. Itemizem Single point of failure in cloud forensics investigation process, because evidence from different servers on the cloud must be stored in central server for investigation process.

5) Lack of international collaboration and legislative mechanism in cross-nation data access and exchange. Specially because cloud forensics depends on collecting evidence from servers located at different countries

6) Integrity and stability, cloud forensics depends on client server communication. Evidence transferred over public network between investigator machine and cloud storage device, integrity of evidence is very important point through investigation process. Many of solutions suggested to enhance the integrity level of cloud forensics investigation process such as in [62], which suggest a digital signature for all collected evidences through evidence collection stage and then check this signature on the other side and when start examination stage. Other solution suggested for this problem by Hegarty [63] which implement a specific framework for digital signature detection that enables forensics analysis of storage platform.

The differences between the investigation of crimes committed in the cloud computing environment and those committed in conventional digital devices are as follows:

1) Conventional digital forensics cannot be used to investigate the incident in cloud computing on the basis of various factors such as the distributed nature of cloud computing [64][65], large resources rather than limited resources in local devices, a large number of data centers located in multiple locations, the presence of third parties and many other factors.

2) Another important factor makes cloud forensics unfriendly and different from digital forensics is that cloud forensics cannot confiscate the suspicious computers and have direct and physical access to the resources that may contain the evidence. This is because all of these evidences are far-reaching and can be found elsewhere.

3) The privacy of user's data, due to the fact that cloud computing contains information from various users, the investigator needs to access total cloud-level data in the data center, user-related information and other users for the purpose of extracting and examining evidence. This process is different and makes cloud forensics uncomfortable from other branches of digital forensics.

4) The nature of cloud computing is complicated, which consist from large number of resources and collect a huge volume of evidence. Based on that a parallel implementation using distributed system is required to enhance the performance of investigation process [66] [67] [50].

5) In general, cloud computing depends on the cloud service provider "CSP" in collecting cloud data, CSP is not a legal investigator, and the trust of cloud service providers is yet another major challenge in implementing digital forensics in a cloud environment that is different to the traditional process of digital forensics investigation.

6) The custody chain differs from that of digital and cloud computing forensics, the custody chain clearly deduces the way evidence has been found, gathered, analyzed and maintained to be submitted to the Court in a manner permissible [11]. In conventional digital forensics, it is trivial to access the history, location, and main resources of the computer. On cloud computing, the location of sources that may contain evidence is hard to identify, because each cloud server is located within a given geographical area, and the time zones for various cloud servers differ.

7) Cloud computing is a system for multiple tenants, while traditional computers are a single owner. This point has a major problem during the investigation, because different users or virtual machines share the same physical resources, and can cause a problem because the investigator has to provide a court with the information collected concerning the suspected user, as the alleged suspect may say that the information contained in the evidence contains data for other users. Another problem here is the privacy of the information of other users, as the investigator can access various user resources.

8) The Cloud Process is limited by Cloud Service Provider and the User-Cloud Provider contract is important because the User-CSP contract includes the Service Level Agreement between the two sides. You could be in an extremely bad situation if this agreement doesn't show at what level your service provider is obliged to provide forensic information, and also how soon it is necessary to do so.

Several investigation frameworks were offered for crimes committed in cloud computing environments, such as the model that was proposed in [68]. A cloud forensics model includes key stages in all models of digital forensics processes such as identification stages, collection stages, preservation stages, examination stages, analyses, and presentations stages. The author develops a proposed model as a service (FPaaS) using cloud-based business process using cloud-based business execution language (BPEL), which combines the four main stages into a single service called (FPaaS). Another model proposed by Shan and Malik [69], which includes three major stages, the identification stage, data collection and preservation stage, and the analytical and presenting stage, is another process model proposed for the cloud computing environment, and, through the suggested model, defines the key challenges which can face each phase within the cloud computer environment.

Martini and choo (2012) [26] suggest a new forensic cloud framework; a proposed model utilizing the main stages of the conventional digital forensics model with enhancement; a principal enhanced point in a model is the iterative stage after the preservation stage, where evidence gathered through the phased evidence is not enough; then the process retraces to the stage of identification. The combination of the two stages of identification, collection and preservation into a unique step is another enhanced feature in the Martini and Cho Framework because evidence can be eliminated or modified at any time in a cloud environment is highly likely to be science and the cloud environment

An Open cloud forensics process model (OCF) was proposed through [70] by Shams Zawoad. This model focuses on the main roles of the cloud service provider, and how the provider effects on the forensics process on the cloud level, and suggest a role of the cloud service provider to support reliable digital forensics in the cloud. Another contribution for this model is to extend the definition of digital forensics investigation process to support reliable digital forensics in the cloud, other contribution for this model that it presents a new architecture which called forensics-aware cloud architecture. The proposed model consists from the basic stage of digital forensics process mode with the addition a verification stage as a last stage of process model.

Table VII shows the key frameworks suggested in a cloud computing environment, the table contains information about each of the key frameworks such as the name of the framework, the contribution for each of the key frame and the goal from proposing each framework, and main stages of the proposed framework by suggesting a set of stage and specific column called other stages if the framework contain stages more than what suggested, and the weak points and drawbacks if exist for each of the listed frameworks. Other process models have been proposed to solve the issues that face the process model of digital forensics when applied in a cloud computing environment. The main challenges facing cloud computing forensics and the solutions proposed to solve them are as follows:

1) The challenges faced by the identification stage are shown in Fig. 4. The first challenge is the access to evidence in log files, which means that it is difficult to access such files in cloud environment due to the fact that there are different formats of log files. Several solutions have proposed to the above challenges in [73], [74], [75], [76], Table VIII shows the main solutions that proposed to deal with the challenges faces the identification stage in the investigation process, Table VIII contain solution name, author name, solution contribution, and solution drawbacks.

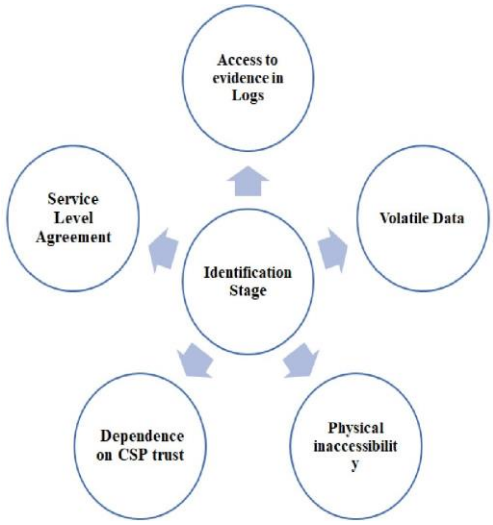

Fig. 4. Major Challenges in Cloud Computing Forensics through the Identification Stage.

The second challenge faced by the identification and collection stage is the volatile data problem. Several solutions have been propose to solve this challenge such solution introduced by Grispos through [77], Grisopos in [77] suggested a new concept to overcome the volatile problem (unstable data) by using a particular strategy that allows the investigators to collect data that may be lost whenever possible. Another solution to volatile data problem proposed by Damshenas and Brik [61], [1] which suggests a frequent data synchronization between virtual machines and persistent storage.

The third challenge confronting the identification and collection stage is the service level agreement "SLA", where "SLA" relates to the primary contract between cloud participant and cloud service provider. This arrangement must include various points that can assist the investigator. The solution to this challenge has been proposed by many researchers as in, [15]. The suggested solution in, [15] comprises a set of conditions to regulate the agreement between the CSP and the participant. Another solution to this challenge proposed by Damshenas [16], And Baset [36]. Their solution comprises a guideline which explains how the SLA should be implemented. In addition to the above solutions, Brik [37] and Haeberlen [78] proposed another solution which suggests a third-party confidence to audit the safety measure given by the CSP.

The fourth challenge in the identification and collection stage is physical inaccessibility due to the nature of cloud computing environment which is geographically spread by the hardware devices as discussed in [62] [79].

The fifth challenge in the identification and collection stage is the dependence on cloud service provider which affects the trust between both CSP and users of the cloud. The absence of transparency and confidence between CSPs and clients is a problem that has been dealt with by Haeberlen [80], which is a primitive fundamental called AUDIT that could be provided by an accountant. Other model called trust cloud framework have been proposed by Ko et al. [81], which consists of five layers of accountability: system, data, workflow, policies, and laws and regulations layers. To increase accountability detective approaches used rather than preventive.

1) The Challenges faced by the analysis stage One of the main challenges faced by the analysis stage is using the encryption algorithms for examination and evaluation stage. In [82] the author proposed a hierarchical attribute- set- based solution to overcome the above challenge. The proposed solution is applied to accomplish fine- grained access control in cloud computing which achieves scalability and flexibility more than confidentiality and authenticity. Another challenge in the achievement of confidentiality and authenticity is through the examination stage. The solution to deal with this challenge was proposed by Prabha N et al. through [83], which presents an encryption technique for query processing on a cloud to protect confidentiality and authentication.

TABLE. VII. MAIN FRAMEWORKS THAT SUGGESTED FOR A CLOUD COMPUTING FORENSICS

FW. Name	Contribution	Identification stage	Evidence Collection	Preservation Stage	Examination and Analysis Stage	Presentation and Reporting Stage	Other Stage	Drawbacks
An integrated digital forensics framework for cloud computing [71]	Define the difference between evidence collection stage and preservation stage in investigation process	✓	✓	✓	✓	✓	x	The main idea of proposed framework is to show that preservation stage is different from collection stage. That's right but a lot of previous work shows that both stages must be at same level to prevent the evidence that collected from any change and update. No any action taken on the other stages of forensics process to be suitable with cloud environment.
Forensics investigation process [57]	A new framework for cloud computing environment with basic change on the main stages of original digital forensic phases	✓	✓	✓	✓	✓	✓	The framework does not take any action for other stages rather than identification stage and collection. The stages of preservation, analysis, examination in digital forensics needs a lot of updates to be suitable for cloud forensics. The author does not take any action in proposed framework to enhance the security and privacy of cloud user's data.
An Open Cloud Forensics model [56]	Main contribution is to run preservation stage in parallel with all other stages of digital forensics stage. Other update added by proposed framework is a combination between examination stage and analysis stage into a new stage called organization stage.	✓	✓	✓	x	x	✓	The author through proposed idea run the preservation stage in parallel with each of original stages of digital forensics, this step will do an overhead on the forensics process because actually it just required in the step of evidence collection, not at each step of forensics process. The author does not add any action to achieve the main principles of security and privacy for user's data on the cloud.
Adams Process model [72]	A new model specified for acquisition stage on cloud computing, define the documents and resources that may contain the evidences that related to the crime.	✓	x	x	x	x	✓	The author proposed an enhanced way for acquisition stage. But no action was taken to enhance other stages to be suitable for cloud computing. The process of enhancement was not completed because the author proposes an enhancement on the level of identification. To complete the process the author must add some enhancement on the level of evidence collection. A lot of principles in the level of security and privacy must be taken into account when trying to design an investigation model which deal cloud computing.
Shah Framework [1]	A new Framework proposed for evidence collection on cloud computing environment, proposed model consist from set of layers, each layer contain set of stages of forensics process model	✓	✓	✓	✓	✓	x	Main drawback in proposed model that this model does not add any specific action on any of digital forensics stages to be suitable with cloud computing environment. The author says that proposed model will deal with the dynamic nature of cloud computing by combining set of stages at same layer, dynamic nature for cloud forensics needs an action to achieve highly level of security on evidence transferring between server and investigator side, and other an action is required to achieve a level of privacy on user's data. The author in his research paper focused on an important issue which faces the process on the investigation in cloud computing this problem is dependent on CSP, no action has been taken by the model to deal with this problem.

TABLE. VIII. MAIN SOLUTIONS THAT PROPOSED TO SOLVE THE ISSUE RELATED TO LOGGING IN IDENTIFICATION STAGE

Solution Name	Author name and year of publish	Contribution for the solution	IaaS	PaaS	SaaS	Drawbacks
Secure logging-as-a-service for cloud forensics [73]	Zawoad S, Dutta AK, Hasan R. SecLaas (2011)	Introduce a secure logging as a service which allow the CSP to store virtual machine logs and provide access to forensics investigators while preserve the confidentiality for the cloud users.	✓	✓	✓	Proposed solution still depends on cloud service provider in the proposed solution, where CSP may not have a level of trust. The other comment is the location of storing VM logs. And how these logs will be stored as clear text or as an encrypted format.
log-based approach to make digital forensics easier on cloud computing [74]	Sang T. A (2013)	Propose a log-based model, the idea of proposed model is to keep another log locally and synchronously. So, it can be used to check the activity on SaaS without interference from CSP. The main goal for this solution is to decrease the interference on cloud service provider on the investigation process. Other goal for proposed solution is to reduce the complexity of the forensics process in cloud computing.	χ	✓	✓	Proposed idea depends on using a SaaS in the cloud side, the user must initiate a request asking for log activity, SaaS will receive the request and then process the request and send it back the response to the user. The process of request and receive a log activity will constitute a great load on the network and will be not secure enough, because there are many of attack in the middle can do sniff and analysis for the traffic because log information must be sent when a small change on the log file happened
Digital forensic readiness in the cloud[75]	Trenwith PM, Venter HS (2013)	The author proposed a model that consider centralized logging for all activities of all participants of the cloud as solution to provide an efficient forensics strategy. Proposed model will enhance and quicken the investigation process.	✓	✓	✓	Main drawback of proposed solution is the centralized location which can have a central point faller, other it is not secure enough when all logs and activities stored at central location. Other main drawback refers to load balancing and heavily traffic on central point
Cloud application logging for forensics [76]	Marty R (2011)	The goal from proposed idea is to provide a lot of information about each record on the log such as when the log happened or record who triggered the event and why it happened, based on that the information that needs to be present at each record will be limited	χ	χ	✓	Proposed idea suggests a log management SaaS to define what is the main field needed at log file, but at the same time it does not provide any solution about logging network usage, file metadata, and other evidence which are important for investigation process in PaaS and IaaS.

2) The multi-tenancy challenge faced by the all stages in investigation process in cloud computing environment. This challenge means that the investigators can access all data of users in the cloud which leads to violate the privacy of users. The solution to this problem was proposed by Aydin M et al. [84]. The solution uses a third party to check and evaluate the data collected by the investigators. Another solution to solve the multi-tenant problem has been proposed by Martini through [26], which proposed a solution depends on upholding the confidentiality and integrity for the evidence that used through the investigation process because the cloud computing environment nature is multi-tenant.

3) The data gathering challenge faced by the acquisition stage: The data is distributed among different servers in cloud computing environment which decrease the performance of the investigation process. The solution to this problem was proposed by Adams in [72] which presents a new cloud forensics model that consists of initial planning stage, on-site survey stage and the acquisition of electronic data.

4) Solution suggested to solve the problem which faces the acquisition stage, Adams in [72] introduces a new cloud forensic model specified for cloud computing environment. The proposed framework specified for evidence acquisition. Not take any action for other stages of forensics process. Proposed model consists from three main stages as follow (a) initial planning stage, which specified for defining and determining all related documents that associated with the investigation, (b) the on-site survey stage, which define all knowledge relating to the location, size, and format of the device that may hold information that can help the investigation process, (c) the acquisition of electronic data which include the process of gathering data related to the crime and store these data. Main drawback for propose that focus on defining and acquiring digital data but does not deal with the stages of analysis and presentation.

IV. CONCLUSION AND FUTURE WORK

Various frameworks and solutions to deal with the process of digital forensics have been proposed. Some of these frameworks and solutions have been proposed as a general framework for digital forensics, while others have been proposed for a particular class of digital forensics such as IoT forensics, network forensics, and other classes. We discussed the main classes of digital forensics through this survey, the major frameworks suggested for each class, the principal steps of each framework, the problems to be solved within the framework, and the major disadvantages of each.

This survey primarily presents and compare between different frameworks suggested for the cloud computing investigation and all other digital forensics classes. We can conclude that most of the frameworks included in our survey focus on solving a specific issue related to CSP, logging issue, or other similar issues. Up to our knowledge we have not

found any framework that takes into consideration the security and privacy issues that are becoming very important issues in cloud computing, especially when dealing with remote servers and cloud participants documentation. In this context, we have recommended a solution to improve many key issues such as security, accuracy, performance and privacy.

REFERENCES

[1] L. Daniel, Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom. Elsevier, 2011.

[2] C. Hargreaves and J. Patterson, "An automated timeline reconstruction approach for digital forensic investigations," Digital Investigation, vol. 9, pp. S69–S79, 2012.

[3] "USLegal-Definitions,"http://definitions.uslegal.com/d/digitalevidence, 2019.

[4] N. T. A. Recipes-A, J. McCaffrey, V. T. Patch, S. Manzuik, P. Chandra, M. Messier, J. Viega, O. D. Wiley, P. Elst, Y. T. Apress et al., "of the book author publisher."

[5] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models international journal of digital evidence," 2002.

[6] M. D. Kohn, M. M. Eloff, and J. H. Eloff, "Integrated digital forensic process model," Computers & Security, vol. 38, pp. 103–115, 2013.

[7] F. Servida and E. Casey, "Iot forensic challenges and opportunities for digital traces," Digital Investigation, vol. 28, pp. S22–S29, 2019.

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

[9] R. McKemmish, What is forensic computing? Australian Institute of Criminology Canberra, 1999.

[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication, vol. 10, no. 14, pp. 800–86, 2006.

[11] J. R. Vacca, Computer Forensics: Computer Crime Scene Investigation (Networking Series), (Networking Series). Charles River Media, Inc., 2005.

[12] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," digital investigation, vol. 7, no. 1-2, pp. 14–27, 2010.

[13] M. Köhn, M. S. Olivier, and J. H. Eloff, "Framework for a digital forensic investigation." in ISSA, 2006, pp. 1–7.

[14] G. Palmer, "A road map for digital forensics research-report from the first digital forensics research workshop (dfrws)," Utica, New York, 2001.

[15] B. Hitchcock, N.-A. Le-Khac, and M. Scanlon, "Tiered forensic methodology model for digital field triage by non-digital evidence specialists," Digital investigation, vol. 16, pp. S75–S85, 2016.

[16] M. Rogers, "Dcsa: Applied digital crime scene analysis," Tipton & Krause, 2006.

[17] S. Von Solms, C. Louwrens, C. Reekie, and T. Grobler, "A control framework for digital forensics," in IFIP International Conference on Digital Forensics. Springer, 2006, pp. 343–355.

[18] H. C. Lee, T. Palmbach, and M. T. Miller, Henry Lee's crime scene handbook. Academic Press, 2001.

[19] S. Ó. Ciardhuáin, "An extended model of cybercrime investigations," International Journal of Digital Evidence, vol. 3, no. 1, pp. 1–22, 2004.

[20] B. Carrier and E. H. Spafford, "An event-based digital forensic investigation framework," in Digital forensic research workshop, 2004, pp. 11–13.

[21] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," in Proceedings of the Fourth Digital Forensic Research Workshop, 2004, pp. 1–9.

[22] M. K. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer forensics field triage process model," Journal of Digital Forensics, Security and Law, vol. 1, no. 2, p. 2, 2006.

[23] S. A. Ali, S. Memon, and F. Sahito, "Challenges and solutions in cloud forensics," in Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing. ACM, 2018, pp. 6–10.

[24] M. Mabey, A. Doupé, Z. Zhao, and G.-J. Ahn, "Challenges, opportunities and a framework for web environment forensics," in IFIP International Conference on Digital Forensics. Springer, 2018, pp. 11–33.

[25] S. Raghavan, "Digital forensic research: current state of the art," CSI Transactions on ICT, vol. 1, no. 1, pp. 91–114, 2013.

[26] J. Yadav, "The impact of digital forensics in future," 03 2017.

[27] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," International Journal of Computer Science and Security (IJCSS), vol. 5, no. 1, pp. 118–131, 2011.

[28] B. Carrier, E. H. Spafford et al., "Getting physical with the digital investigation process," International Journal of digital evidence, vol. 2, no. 2, pp. 1–20, 2003.

[29] R. Van Baar, H. Van Beek, and E. Van Eijk, "Digital forensics as a service: A game changer," Digital Investigation, vol. 11, pp. S54–S62, 2014.

[30] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, vol. 9, no. 2, pp. 71–80, 2012.

[31] D. Quick and K.-K. R. Choo, "Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive," Trends & Issues in Crime and Criminal Justice, vol. 480, pp. 1–11, 2014.

[32] A. Yasinsac, R. F. Erbacher, D. G. Marks, M. M. Pollitt, and P. M. Sommer, "Computer forensics education," IEEE Security & Privacy, vol. 99, no. 4, pp. 15–23, 2003.

[33] A. Al-Dhaqm, S. Razak, S. H. Othman, K.-K. R. Choo, W. B. Glisson, A. Ali, and M. Abrar, "Cdbfip: Common database forensic investigation processes for internet of things," IEEE Access, vol. 5, pp. 24 401– 24 416, 2017.

[34] E. Benkhelifa, B. E. Thomas, Y. Jararweh et al., "Framework for mobile devices analysis," Procedia Computer Science, vol. 83, pp. 1188–1193, 2016.

[35] M. Petraityte, A. Dehghantanha, and G. Epiphaniou, "Mobile phone forensics: an investigative framework based on user impulsivity and secure collaboration errors," in Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. Elsevier, 2017, pp. 79–89.

[36] H. Dreger, A. Feldmann, M. Mai, V. Paxson, and R. Sommer, "Dynamic application-layer protocol analysis for network intrusion detection," in 15th USENIX security symposium. USENIX Association, 2006, pp. 257–272.

[37] G. Maier, R. Sommer, H. Dreger, A. Feldmann, V. Paxson, and F. Schneider, "Enriching network security analysis with time travel," in ACM SIGCOMM Computer Communication Review, vol. 38, no. 4. ACM, 2008, pp. 183–194.

[38] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the internet of things: A survey," in 2016 Cybersecurity and Cyberforensics Conference (CCC). IEEE, 2016, pp. 28–34.

[39] K. Shanmugasundaram, N. Memon, A. Savant, and H. Bronnimann, "Fornet: A distributed forensics network," in International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, 2003, pp. 1–16.

[40] W. Wang and T. E. Daniels, "A graph based approach toward network forensics analysis," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 1, p. 4, 2008.

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

[42] C. Prosise, K. Mandia, and M. Pepe, "Incident response & computer forensics," 2003.

[43] R. Geambasu, T. Bragin, J. Jung, and M. Balazinska, "On-demand view materialization and indexing for network forensic analysis." in NetDB, 2007.

[44] A. Singhal, C. Liu, and D. Wijesekara, "Poster: A logic based network forensics model for evidence analysis," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 1677–1677.

[45] M. Neugschwandtner, P. M. Comparetti, G. Jacob, and C. Kruegel, "Forecast: skimming off the malware cream," in Proceedings of the 27th Annual Computer Security Applications Conference. ACM, 2011, pp. 11–20.

[46] U. Bayer, P. M. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, behavior-based malware clustering." in NDSS, vol. 9. Citeseer, 2009, pp. 8–11.

[47] T. Tafazzoli, E. Salahi, and H. Gharaee, "A proposed architecture for network forensic system in large-scale networks," arXiv preprint arXiv:1508.01890, 2015.

[48] L. Jiang, G. Tian, and S. Zhu, "Design and implementation of network forensic system based on intrusion detection analysis," in 2012 International Conference on Control Engineering and Communication Technology. IEEE, 2012, pp. 689–692.

[49] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in 9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing. IEEE, 2013, pp. 608–615.

[50] M. H. Qasem and M. Qatawneh, "Parallel hill cipher encryption algorithm," International Journal of Computer Applications, vol. 179, no. 19, pp. 16–24, 2018.

[51] A. MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the ioa era," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2018, pp. 1–5.

[52] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2016, pp. 356–362.

[53] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "Iotdots: A digital forensics framework for smart environments," arXiv preprint arXiv:1809.00745, 2018.

[54] A. Nieto, R. Rios, and J. Lopez, "A methodology for privacy-aware iot-forensics," in 2017 IEEE Trustcom/BigDataSE/ICESS. IEEE, 2017, pp. 626–633.

[55] "Iot-forensics meets privacy: towards cooperative digital investigations," Sensors, vol. 18, no. 2, p. 492, 2018.

[56] T. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in internet of things (iot)," in Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM, 2017, p. 55.

[57] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," Digital Investigation, vol. 10, no. 1, pp. 34–43, 2013.

[58] C. Esposito, A. Castiglione, and K.-K. R. Choo, "Challenges in delivering software in the cloud as microservices," IEEE Cloud Computing, vol. 3, no. 5, pp. 10–14, 2016.

[59] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," Digital Investigation, vol. 13, pp. 38–57, 2015.

[60] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in IFIP International Conference on Digital Forensics. Springer, 2011, pp. 35–46.

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

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

[63] R. Hegarty, M. Merabti, Q. Shi, and B. Askwith, "Forensic analysis of distributed data in a service oriented computing platform," in proceedings of the 10th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PG Net, 2009.

[64] M. Rajallah Asassfeh, M. Qatawneh, and F. Alazzeh, "Performance evaluation of blowfish algorithm on supercomputer iman1," International journal of Computer Networks and Communications, vol. 10, pp. 43–53, 03 2018.

[65] M. Alkhanafseh and M. Qatawneh, "A parallel chemical reaction optimization algorithm for max flow problem," International Journal of Computer Science and Information Security,, vol. 15, pp. 19–32, 06 2017.

[66] H. Harahsheh and M. Qatawneh, "Performance evaluation of twofish algorithm on iman1 supercomputer," International Journal of Computer Applications, vol. 179, pp. 1–7, 06 2018.

[67] A. Al-Shorman and M. Qatawneh, "Performance of parallel rsa on iman1 supercomputer," International Journal of Computer Applications, vol. 180, pp. 31–36, 04 2018.

[68] A. Eleyan and D. Eleyan, "Forensic process as a service (fpaas) for cloud computing," in 2015 European Intelligence and Security Informatics Conference. IEEE, 2015, pp. 157–160.

[69] J. Shah and L. G. Malik, "An approach towards digital forensic framework for cloud," in 2014 IEEE International Advance Computing Conference (IACC). IEEE, 2014, pp. 798–801.

[70] S. Zawoad, R. Hasan, and A. Skjellum, "Ocf: an open cloud forensics model for reliable digital forensics," in 2015 IEEE 8th International Conference on Cloud Computing. IEEE, 2015, pp. 437–444.

[71] M. Hogan, F. Liu, A. Sokol, and J. Tong, "Nist cloud computing standards roadmap," NIST special publication, vol. 35, pp. 6–11, 2011.

[72] R. Adams, "The advanced data acquisition model (adam): A process model for digital forensic practice," Ph.D. dissertation, Murdoch University, 2012.

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

[74] T. Sang, "A log based approach to make digital forensics easier on cloud computing," in 2013 Third International Conference on Intelligent System Design and Engineering Applications. IEEE, 2013, pp. 91–94.

[75] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," in 2013 Information Security for South Africa. IEEE, 2013, pp. 1–5.

[76] R. Marty, "Cloud application logging for forensics," in proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 178–184.

[77] G. Grispos, T. Storer, and W. B. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics," International Journal of Digital Crime and Forensics (IJDCF), vol. 4, no. 2, pp. 28–48, 2012.

[78] "Computer Forensics: Network Forensics Analysis and Examination Steps,"https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/network-forensics-analysis-and-examination-steps/#gref., 2019.

[79] K. Ruan, "Cybercrime and cloud forensics: Applications for investigation," 2013.

[80] A. Haeberlen, "A case for the accountable cloud," ACM SIGOPS Operating Systems Review, vol. 44, no. 2, pp. 52–57, 2010.

[81] R. K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," in 2011 IEEE World Congress on Services. IEEE, 2011, pp. 584–588.

[82] S. Gokuldev and S. Leelavathi, "Hasbe: A hierarchical attribute- based solution for flexible and scalable access control by separate encryption/decryption in cloud computing," International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 2, no. 3, 2013.

[83] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Cloud log forensics: foundations, state of the art, and future directions," ACM Computing Surveys (CSUR), vol. 49, no. 1, p. 7, 2016.

[84] M. Aydin and J. Jacob, "A comparison of major issues for the development of forensics in cloud computing," in 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). IEEE, 2013, pp. 77–82.