I.J. Wireless and Microwave Technologies, **2020, 5, 1-12**
Published Online October 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2020.05.01

Cloud Forensics: Challenges and Blockchain Based Solutions

Omi Akter[a], Arnisha Akther[b], Md Ashraf Uddin[c], Md Manowarul Islam[d]
[a]Dept. of EEE, Chittagong University, Chittagong, Bangladesh
[b,c,d]Dept. of CSE, Jagannath University, Dhaka, Bangladesh
Email: [a]omiaktercu@gmail.com, [b]arnisha@cse.jnu.ac.bd, [c]ma.uddin@federation.edu.au, [d]manowar@cse.jnu.ac.bd

Received: 11 March 2020; Accepted: 20 July 2020; Published: 08 October 2020

Abstract: With the advancement in digital forensics, digital forensics has been evolved in Cloud computing. A common process of digital forensics mainly includes five steps: defining problem scenario, collection of the related data, investigation of the crime scenes, analysis of evidences and case documentation. The conduction of digital forensics in cloud results in several challenges, security, and privacy issues. In this paper, several digital forensics approaches in the context of IoT and cloud have been presented. The review focused on zone-based approach for IoT digital forensics where the forensics process is divided into three zones. Digital forensics in cloud provides the facilities of large data storage, computational capabilities and identification of criminal activities required for investigating forensics. We have presented a brief study on several issues and challenges raised in each phase of Cloud forensics process. The solution approaches as well as advancement prospects of cloud forensics have been described in the light of Blockchain technology. These studies will broaden the way to new researchers for better understanding and devising new ideas for combating the challenges.

Index Terms: Cloud Digital Forensics, Challenges, Digital Forensics, Forensics Tools, Blockchain, IoT, Solutions.

1. Introduction

The dependency on the cyberspace particularly on the internet has been dramatically increased nowadays. The advancements in the technology is giving rise to the latest paradigms like fog, cloud computing where Cloud computing is one of the most widely used paradigm at the present time. Cloud computing has been given rise to several economic opportunities and promising technologies that become the most important and evolutionary part in latest computing era. This paradigm has enabled the capability to store large amount of data privately and helps to provide the data security over the internet. In case of large scale of cloud data storage, it would be very tedious task to investigate the data on the cloud if an attacker attacks on cloud network. Thus, a latest discipline called digital Cloud forensics has been introduced in the recent years. Cloud forensics involves the growing use of networks, digital devices for storage, and computers in identification of several criminal activities being performed in both Hi-Tech and traditional forensics [1]. The traditional digital forensics process is integrated with Cloud-based technologies which are often referred to as Cloud forensics. In short, cloud forensics is the combination of digital forensics with cloud computing. Cloud forensics is an application inside the framework of digital forensics which identifies the crimes performed on the cloud and performs the required investigation with minimum overhead and complications [2]. Several categories of digital forensics such as computer forensics, network forensics, mobile device forensics, digital image forensics, digital audio forensics and memory forensics have been developed over the years. The traditional processes of forensic investigation are less effective and efficient due to the decentralized processing of data [3]. Thus, to overcome these limitations of traditional process, the digital forensics is integrated with cloud. The cloud computing evolution poses several challenges and issues mostly in digital forensics and crime investigation. The investigation process for any kinds of platform includes several phases such as- identification of problem, data collection, examination of crime scenes, and analysis of the investigation and presentation of the case findings [4]. The studies done by various researchers have shown that the implementation of Cloud based digital forensics is complex and several issues and challenges are involved in every stage of Cloud forensics. The review presented here includes a detailed study on several issues and challenges faced in each phase of cloud forensics process. Some of the Cloud forensics related issues are accessing logs, collecting stable data, huge amounts of data, recreation of the crime scenario, multi-national laws, presenting evidences in court etc. Some solutions such as maintaining logs, separate plane for cloud data retrieval and legislative solutions are suggested in the paper.

Since Cloud forensics is a growing interesting field in research, we focus to conduct a thorough analysis on the issues and challenges of cloud forensics based on the existing literature to present an analytic review. A few recent scientific papers retrieved from well-known academic databases are taken for consideration. This paper identifies the major challenges, existing solutions, and open problems in the field of cloud forensics based upon the outcome of the review.

In this paper, we review the cloud based digital forensics which includes the concept of cloud digital forensics, the IoT based approaches in digital forensics, the issues and challenges existing in the cloud based approach and the possible Blockchain solutions to the problems. Recently, Blockchain has been regarded as a promising technology for the preservation and tracking of the Chain of Custody in digital forensics. Blockchain, a linear data structure enables all interested stakeholders to create a digital ledger for documenting and storing transactions (events / records) exchanged over a distributed network of computers. This structure of the Blockchain can potentially guarantee the security and privacy of digital evidence for conducting cloud forensics.

In section 2, the various methodologies and frameworks used in the conventional cloud-based forensics are reviewed. Section 3 contains Cloud forensic approached based on IoT, types of evidences and the importance of cloud in digital forensics. In section 4, various security issues and challenges on the different stages of Cloud forensics process has been evaluated. In section 5, possible solutions with respect to traditional and Blockchain technology for the identified challenges and issues have been presented. The last section concludes the findings of the reports with their possible works that can be done in the future.

2. Traditional Cloud Forensics in literature

Harbawi et al. [2] focused on the digital evidence which plays a crucial role in cyber-oriented and electronic crimes and it is considered as a key point for the process of digital forensic analysis. To improve the existing digital security of IoT forensics, an improved and theoretical framework was provided. LoS algorithm deployment which is the most improved procedure was introduced in the paper. This algorithm enhances traceability and decreases the complications and overhead in the analysis of digital forensics. A concept of management platform has also been proposed in the system to maximize advantages of experienced forensic cases based on IoT and an outline for its optimal implementation is also represented in the paper. Oriwoh et al. [5] presented the comparison between traditional and IoT based forensics and it has been concluded that IoT forensics is more efficient and effective. To improve IoT based DF, the paper introduced two aspects: applications of 1-2-3 Zones method to Digital Forensics investigation based on IoT and NBT (Next-Best-Thing Triage) that can be used with integration of 1-2-3 Zones method. The authors concluded that the approaches introduced in the paper are necessary for IoT based DF. The approaches are proposed to increase the effectiveness and efficiency of IoT DF by ensuring the relevant evidence acquisition and identification and by maximizing use of available time. Pichan et al. [3] studied that existing traditional approaches are not practically possible due to decentralized processing of data. Thus, this paper reviewed issues in implementation of cloud computing in each phase of traditional digital forensic. The paper also represented the recent developments in cloud based forensic done by Amazon and NIST. Simou et al. [4] presented the digital forensic process based on cloud which includes identification, collection, analysis, and presentation stage. The stages have been categorized based on frameworks and models proposed by the industry and academics. The results of the study represented an overview of challenges and issues faced in the implementation of each phase of cloud forensics. Dykstra et al. [6] presented two hypothetically case studies a compromised website based on cloud and child pornography on the cloud. The study described the most significant challenges in cloud DF which include evidence preservation, chain of custody and forensic acquisition. Daryabar et al [7] focuses on the increasing of cloud computing in today’s world and the impact of cloud technologies on digital forensics. The study performed a literature review on challenges including privacy and security issues, customer, and trust issues etc. in digital forensic investigation based on cloud computing and analyze and evaluate basic architecture and framework of DF and with cloud computing. Simou et al [8]. Represented the methodological aspects and the frameworks being used in cloud forensics and it critically reviewed the existing issues in implementation of cloud forensics stages and the possible solutions to the issues. A detailed comparison has represented the similarities and limitations between existing methodologies. The review is performed to understand the basic requirements of investigators during forensic process. Pandi et al. [1] reviewed forensic architecture based on cloud environment that provides the challenges and the solutions to those challenges. The paper has presented the various categories in digital forensics with its investigation process. A comparison on different frameworks of cloud forensics introduced by various authors has been discussed. The detailed study has revealed the advantages and limitations of prevailing methods in cloud forensics with some creative exploration guidelines and has given a brief on India Cyber Laws. The results show that the existing frameworks of digital forensics are not supporting cloud environment efficiently; thus, a standardized framework should be built up to enhance the forensic investigations. Sonone et al. [9] provided a better awareness towards cloud forensics by understanding the various proposed frameworks, the essential components in cloud architecture, possible attacks on the cloud services, types of forensic approaches i.e. digital forensics, computer forensics, network forensics and cloud forensics and identifying the challenges and research gaps in cloud based forensics. The paper has represented a state-of-art that will be beneficial to researchers and practitioners in future research related to cloud forensics. The summary of the above state-of-the-art works has presented in Table 1.

Table 1. The summary of literature review

Author name	Findings
Harbawi et al. [2]	The authors proposed an improved and theoretical framework to enhance the security of existing digital forensics and introduced LOS algorithm to decrease the complications in forensics process.
Oriwoh et al. [3]	The authors compared between traditional and IoT based forensics process. Two aspects related to 1-2-3 Zones were represented that improved the effectiveness and efficiency of IoT DF.
Pichan [4]	They highlighted the least possibility of traditional approached due to decentralized data and reviewed the challenges that exist in each phase of cloud computing.
Simou et al. [5]	They reviewed the four stages in digital forensics process. The stages are divided according to frameworks and models. They also discussed the challenges and issues in cloud forensics.
Dykstra et al. [6]	Two hypothetical cases studies to understand the criminal targets and challenges in digital forensics have been reviewed.
Daryabar [7]	The authors represented a review on various types of challenges and evaluated the basic architecture and framework of DF with and without cloud computing.
Simou [8]	The research represented methodological aspects and frameworks and the comparison between existing methodologies.
Pandi et al. [1]	The study reviewed the challenges and solutions to the forensic architecture and the appropriate solutions to those challenges. The various forensics categories are also discussed in the paper.
Sonone [9]	They provided better awareness towards cloud forensics which included cloud architecture, types of forensic approaches and challenges etc.
Liu et al. [10]	They identified evidence for Cloud Forensic analysis. A Prolog-based analysis tool was executed by studying the signals from various setups.
O’Shaughnessy et al. [11]	They studied the consequence that cloud computing possesses on conventional digital forensic analyses.
Sandez et al. [12]	They reviewed technical problems while investigating Cloud Based Environments.

3. Cloud Forensics

In this section, we first describe different steps of the cloud forensics, traditional vs cloud forensics, the significance of cloud forensics, digital forensics approach in IoT, different kinds of evidences collected in IoT, the importance of cloud forensics and cloud forensics tools. A digital forensic crime scene investigation including mobile, fog and cloud is involved several steps illustrated in Fig 1: The first step of conducting digital forensics involves four activities listed below.

- Identification: The first step in computer forensic in identification of the case and it involves two main steps as evidence and incident identification, which will be helpful to prove the incident that has happened in the case scenario.
- Collection and Preservation: The second step is the collection of evidence from different digital devices like cell phone, e-mails, hard disk, and any other different types of digital media and secures the evidence for further process with integrity of the evidence.
- Examination and Analysis: The third step is organizing the evidence and it involves analysis and examination of the devices for evidence as digital clues. Firstly, the investigator extracts the information for examination of the case and inspects the extracted data and their characteristic. Secondly, in analysis part, the investigator interprets and correlates the data to know the fact and draw conclusion whether the evidence is proved or not.
- Presentation: Finally, the investigator prepares the reports from the findings about the findings of the investigation and makes it appropriate enough with evidence to finally present it to the court.

The second step is the custody of chain (CoC) which refers to the sequential process of collecting data, whether it be physical or electronic in legal cases. The chain should be recorded for any forensic case to demonstrate the end to end sequence of research performed, including by whom, when (i.e. date/time), and intention.

The last step of digital forensics is called documentation which is a continuous process throughout the investigation process. Precisely recording location and status of electronic devices, storage media, and other traditional evidence are paramount for future investigation.

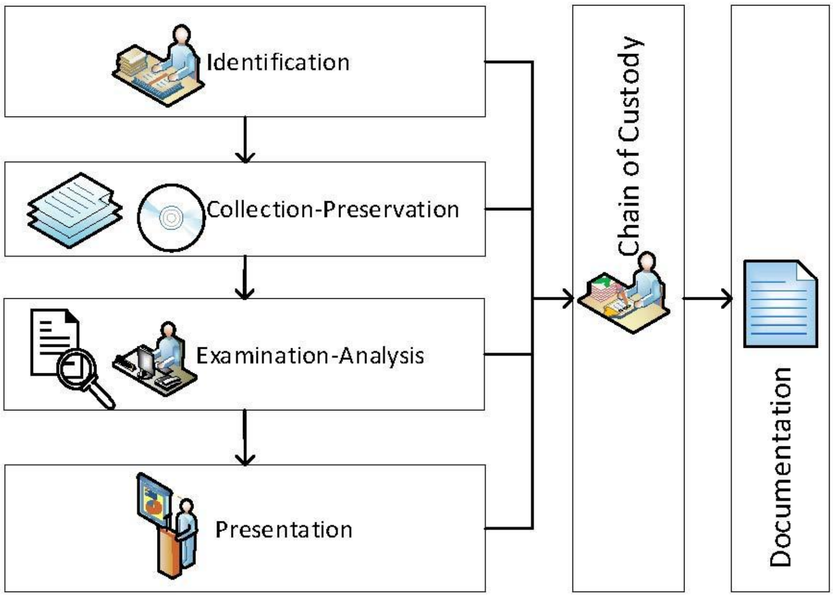

Fig. 1. Digital forensics process flow for investigation

3.1 Traditional Forensics vs Cloud Forensics

In traditional, the investigator controls the evidence but in cloud, it depends on various cloud service providers. Digital Forensic is characterized as the utilization of experimentally incidental and demonstrated strategies for the identification, validation, interpretation, collection, preservation, presentation and documentation of the evidence collected from the digital devices got from advanced hotspots to encourage or assisting the recreation of occasions saw as criminal, or predicting unapproved activities demonstrated to be problematic to arranged tasks[17].

Cloud computing is a model for empowering pervasive, helpful, on-request system access to a common pool of configurable computing properties (e.g. systems, servers, storing, applications and administrations) that can be quickly provisioned and discharged with insignificant administration exertion or specialist organization collaboration[18].

Accordingly, cloud crime scene investigation can be characterized as the utilization of established techniques for the safeguarding, gathering, approval, distinguishing proof, examination, translation, documentation and introduction of advanced proof from dispersed registering frameworks in a way that keeps up the trustworthiness of the proof so it is acceptable in an official courtroom[19].

A computerized scientific procedure model gives a structure to leading sound criminological examinations[17].While there is no advanced measurable procedure model that is fit to all computerized criminological examinations, a conventional procedure model can be applied to a wide range of kinds of advanced scientific examinations paying little mind to the innovation that is utilized.

3.2 Significance of Digital Forensics in Cloud Computing

Cloud Computing has transformed the way IT performs, it has changed the way IT services are created, managed, performed, and outsourced. Cloud forensics is a new dimension in computing which has several importance and significance in digital forensic [20] as listed below.

- **Cost effectiveness and data abundance:** Cloud computing provides client with unlimited memory capacities; we can store large volume of digital evidence in the Cloud which costs lower compared to the off-premise physical memory.
- **Flexibility**: Cloud computing is more flexible because it provides access to digital evidence in and out of workplaces. Anyone can access the cloud forensics resources from anywhere by using laptops, cell phones or any other web based digital devices.
- **Efficiency:** The forensics experts can focus on the fundamental issues of conducting forensics while leaving the task of running IT infrastructure to the cloud service providers.
- **Security Features:** Policies, standard and procedure of cloud computing enables the forensics experts with special security and the users will rely on cloud.
- **No hardware Requirement:** The forensics experts do not require physical hardware to run the forensics tools, rather cloud runs those efficiently.
- **Policies and standard:** Cloud computing maintains standard and policies as per their requirement to conduct sensitive activities of digital forensics.

3.3 Digital forensics approaches for IoT

The investigation processes in the case of any crime scene involving the use of Internet of Things (IoT) devices is done using some standardized approaches in order to provide a proper mechanism for finding the evidence which is presentable in the court proceedings [2]. Every forensic approach used in the IoT environment generally follows some common steps of investigation. These steps are defining the scenario related to the problem, collecting related data, investigating crime scenes, analysing the evidences, and finally documenting the case. The digital forensics process flow is depicted in Fig 1.The various approaches that are available for digital forensics investigation are Extended Model of Cybercrime Investigation (EMCI), Abstract Digital Forensic Model (ADFM), and Digital Forensic Research Workshop (DFRW) [10]. The investigations in IoT cases require the points where the evidence is to be looked. One approach to find such places is zone-based approach as depicted in Fig 2. The whole scenario is divided into three zones. The first zone is the internal network which involves all the wireless devices and sensors and the data regarding their working states. The second zone involves the network devices that sit at the fence of the internal network. These devices are typically network firewalls and Intrusion Detection Systems (IDSs). The third zone involves all the devices present on the public network like Internet Service Provider, web services, clouds etc. [5].This work also initiates a Next-Best-Thing Triage (NBT) Model for use in harmony with the 1-2-3 Zones approach in essential occurrences and vice versa. The DF process from an IoT perspective require these two 'approaches': the atypical nature of IoT sources of evidence (i.e. Objects of Forensic Interest - OOFI), the insidiousness of the IoT environment and its other unique attributes. The amalgamation of these attributes utters the necessity for a systematic DF approach to occurrences. Direct access to Objects of Forensic Interest (OOFI) may not always be possible within the IoT domain (or appropriate e.g. pacifiers). That is the reason behind proposing the Next Best Thing Triage (NBT) model of approaching IoT investigations. However, in these circumstances, identification and considering the next best source of relevant evidence is required. Further researches may find ways to design a method of systematically deciding what this next best thing.

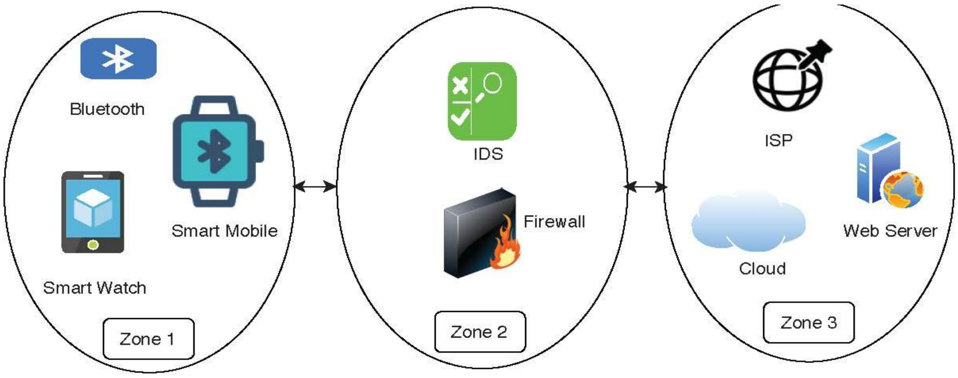

Fig. 2. Zonal approach in IoT forensics

3.4 Types of Evidence in Cloud of Things

Digital forensics is applied in different area as depicted in Fig 3. The investigation of a crime scene which involves Internet of Things (IoT) may encounter many types of devices including various electrical appliances like computers, washers, and mobile phones. The forensics in Cloud platform requires combining all technologies of different digital forensics area. The different types of devices in an IoT crime investigation scenario present many challenges in the investigation process. The concept of various types of technologies interacting with each other is seen in our surroundings like the connection of various neurons in our brain [11]. The number of devices that are present in a traditional digital forensics' investigation is much lesser than the same in the case of IoT digital forensics. The amount of data is going to increase exponentially with the introduction of IoT in the society as the many devices will be connected to the internet including the simple devices that are used in the routine lives of people [12]. The anticipated increase in the amount of data from 2005 to 2020 is about 40,000 trillion gigabytes [13]. With the increase in number of devices, the boundary between the Local Area Networks (LANs) and Wide Area Networks (WANs) is going to fade away.

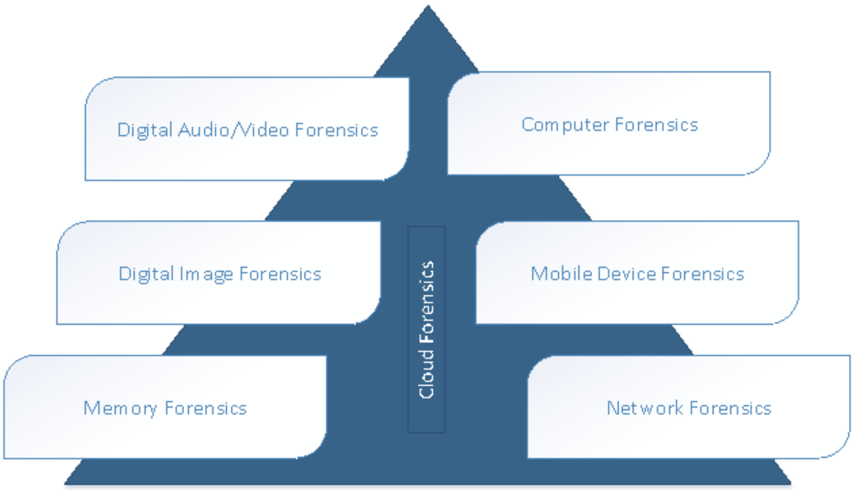

Fig. 3. Categories of forensics

3.5 Importance of cloud forensics

The cloud computing paradigm is becoming more and more popular and is revolutionizing the way various Information Technology (IT) services work. The increase in the scale of cloud computing has been increasing at a very fast pace and is expected to increase more in the future. There is one aspect of cloud computing which is always in the minds of the consumers and that is the storage of private user data on cloud servers with proper security. Another factor involving the cloud computing is its use in various cyber thefts and crimes. The power that cloud computing provides in terms of computational capabilities and storage, is very big and can be used to perform various malicious activities online. Attackers can disappear after performing attacks using cloud servers and cannot be traced easily [3]. The various forensic approaches that are used in traditional systems cannot be applied to the cloud computing as in the latter case, the evidences are present on a virtual instance inside the storage of a distant server which is storing a vast number of instances for a very large number of users. The instances are difficult to be traced along with their users. In such cases, there is a need to design strategies for investing cases involving cloud computing.

3.6 Forensics Tools

Some forensics tools and their description are illustrated in Table 2 and 3. Table 2 illustrates the tools of traditional forensics and Cloud Forensics. Table 3 describes the tools in the context of the types of forensics including memory forensics, mobile device forensics, and software forensics.

Table 2. Traditional and cloud forensics tools

Traditional Forensic Tools	**Cloud Forensic Tools**
FTK Imager	E-Discovery by Access Data
Prodiscover	E-Discovery by Encase
SANS SIFT	OWADE, (Offline Windows Analysis and Data Extraction).
Mandiant RedLine	BlackBag or Cellebrite

Table 3. The summary of digital forensics tools

Forensics Tools	Description
Digital Forensics	It is used for retrieving evidences from computer. It comprises of preservation, identification, data retrieval etc. which includes the standards of computer forensics. Examples: Forensics toolkit, SANS Investigative Forensics Toolkit
Memory Forensics	It is used to find out the possible remains in the computer memory at that time when no data has been left on hard drive or it has been erased knowingly. For examples, Volatility, Windows SCOPE etc.
Mobile Devices Forensics	As the name suggests that it comprises the evidences which are found on mobile or any mobile devices as now-a-days communication has made lot of advancement in portable devices. For example, XRY, Magnet AXIOM etc.
Software Forensics	It helps to find out whether the software has been stolen by making comparison of source code and this tool is used for many high-profile litigations related to intellectual property. For example, Code Suite.

4. Issue and challenges in Cloud Forensics

In this section, we describe the issues and challenges that exist in cloud forensics.

4.1 Cloud forensics issues

There are some issues in the cloud forensics approaches and models due to the highly remote nature of cloud computing. Some of the issues are listed in this section.

- **Accessing Logs:** The general computer investigation approach to trace a cybercrime involves finding the logs of each activity on the devices and then analyzing them to find the evidences. Cloud computing paradigm is different in this context as the logs are in an unknown server in a distant place. The process of accessing logs becomes very difficult in cloud computing [4].
- **Collecting stable data:** The data collection mechanism is designed so that the evidences contain stable data which is presentable in the court. The preservation of stability of data is very difficult in cloud computing as it is of very volatile nature due to the presence of multiple users sharing same physical space [5].
- **Huge amount of data:** Another big issue in cloud forensics is the presence of large amounts of data which are to be analyzed in order to find the evidences. The tools used for traditional forensics are not compatible with such large amounts of data. The investigation processes require the cooperation of the Cloud Service Provider (CSP)[6].

4.2 Challenges in Cloud Forensics

The cloud forensics approaches, and investigation models require some challenges to be faced in order to finalize the results of the investigations [14]. Some of these challenges are listed in this section.

- **Recreation of the crime scenario**: The investigation approaches sometimes require the recreation of the whole criminal activity in order to trace the evidences. This process involves the repetition and simulation of all the activities performed in the crime scene. Cloud computing poses problems in doing this as clouds are stored as virtual instances which can be deleted after the crime leaving no trace and room for recreation [14].
- **Multi-national laws:** The investigations are done following the laws of the countries in which the criminal activities are performed. In case of cloud forensics, the cloud data centers are located world-wide and hence multiple laws are to be followed for proceeding the investigations [15].
- **Presenting evidences in court:** The presentation of the found evidences in court is required for the case investigations. Jury members may not have the knowledge of the complex structure of cloud computing models. Due to this reason, evidence presentation becomes a difficult task in cloud forensics [16].
- **Crime Scene Reconstruction:** Often the investigators must reconstruct the crime scene in order to investigate the malicious activity [17]. In traditional digital forensics, the investigator can identify the number of devices used in the crime or the people involved in the crime easily [21, 22]. The cloud context, however, implies real-time and autonomous interaction between various nodes, which makes it almost impossible to reconstruct the crime scene and to identify the scope of the damage, due to the highly dynamic nature of the communication.
- **Evidence Segregation:** In the cloud, using virtualization, different instances running on a single physical machine are isolated from each other [21]. Since the multiple users behave like they are running on the separate host although they data instances are stored same machine. So, it is a quite impossible for CSPs and law enforcement agencies to separate them during the investigations without breaking the confidentiality of others that share the infrastructure.
- **Lack of User Information/IP Anonymity:** In clouds, most of the service providers maintain user-friendly policies and require minimal information from the user [22, 24]. As results, it is challenging for the investigator to track the criminal using the minimum information provided from limited user information.
- **Data Origin:** Unlike the usual digital forensics examinations, in clouds there is less certainty about where the data came from, as data may come from any possible location from thousands of users locations and it is quite difficult to identify who or what created and/or modified the data object in the clouds[22].
- **Data Protection and Lack of Transparency in Cloud Services:** Most of the cases, storage and data protection are typically performed by the IaaS vendor like Google Cloud, AWS, Microsoft Azure, iCloud, and many more [22][23]. However, many providers use common keys for storage encryption and archiving.
- **Less Control in Clouds:** In cloud forensics, the access level of the investigator on cloud devices are depend on the different service models compared to the digital forensics where the investigator has full access of the devices [22].

5. Cloud Forensics Solution

We have already discussed some of the challenges that are present in cloud forensics models. There is a lot of conventional work done in addressing these challenges. We discussed two kinds of solutions: Traditional solutions and Blockchain based solutions.

5.1 Traditional Solutions

- **Maintaining logs:** The log maintenance is a major issue in cloud computing as discussed earlier. There are some proposed models for maintaining logs in cloud computing. One proposed solution is to store logs of each activity that changes the state of the instance and then transferring the logs to a central log storage cloud using special transport layer protocols created for the task [15].
- **Separate plane for cloud data retrieval:** The challenge of data collection in cloud forensics can be mitigated by providing a separate plane for managing the data retrievals required by the investigators. This plane of cloud infrastructure must be maintained by trustworthy parties [16].
- **Legislative solutions:** The solution to the problem of lack of robust laws for cloud forensics is to have a concrete Service Level Agreement (SLA) between the customers and the cloud service providers (CSPs) which states the laws to be followed in the case of criminal investigation procedures [6].

5.2 Blockchain based Solutions for Cloud Forensics

Blockchain has recently emerged a breakthrough technology to ensure higher security and privacy in many applications including eHealth [28-30], IoT [27] [31], industries, voting [32]. Blockchain refers to a decentralized, shared, and tamper-proof ledger which is replicated on a peer-to-peer network as depicted in Fig. 4(a). The Blockchain was first successfully used in bitcoin which is a virtual cryptocurrency system [33]. The basic data unit of the Blockchain is called transactions. A certain number of transactions are bundled in a Block. The Blockchain nodes broadcasts the Block for generating target hash code for the Block. This process is called Proof of Work [34][35] as shown in Fig. 4(c). The Blockchain technology can promote the current Digital Forensics and Incident Response (DFIR) if it is incorporated into the current forensics system [36]. Logs created by IoT devices and Cloud server can aid in the reconstruction of events, but their credibility and therefore admissibility can only be accomplished if a chain of custody (CoC) is preserved on the Blockchain based digital forensics system. The tamper-proof, distributed nature of the Blockchain has inspired researchers to device Blockchain assisted Cloud forensics framework. In this paper, we presented few recent works on Blockchain enabled Cloud forensics to address the Cloud forensics challenges.

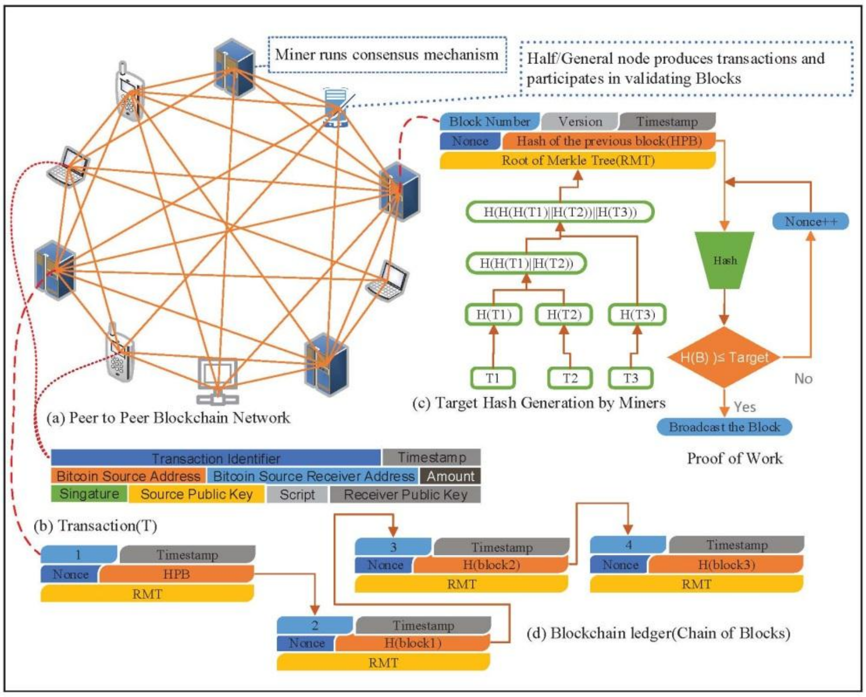

Fig. 4. The components of a bitcoin Blockchain (adapted from [27])

The major problems considered in cloud forensics are storage of evidence and the integrity of evidence. The authors in [37] suggest a blockchain-based data storage and integrity management framework for cloud forensics to solve these problems. Therefore, it compares the efficiency of the proposed network with the other cryptocurrencies based on blockchain. The framework proposed would guarantee data integrity when handling more transactions than current permission-less-based blockchains. Nonetheless, there is a drawback that the current system's output assessment cannot perform the actual assessment simply by comparing the measured outcome values by measuring the predicted data size. Network data is collected with snort to carry out simulation and calculate tps using Hyperledger for future extension of this work. Another work in [38] proposes a digital evidence processing system based on blockchain IoT. Leveraging the blockchain technology, permitted IoT forensics system centered on blockchain is proposed to enhance the credibility, legitimacy, and non-repudiation properties of the collected proof. The device architecture is explicitly described, information of the mechanism is provided and a cryptographic-based solution to alleviate privacy concerns about identity is introduced. Taking advantage of smart contract, various types of transactions suitable for this forensic application are established. To tackle the question of identity privacy further, a changed Merkle signature scheme to conceal from the public the identity of the submitter of proof is used. One potential future work is to integrate the system into an IoT testbed containing a heterogeneous set of devices, to test the reliability of the system and to benchmark the results.

In the Internet of Things (IoT) and social networks climate, a novel blockchain-based DF investigation platform is proposed [39] which can provide proof of presence and privacy for proof items analysis. To incorporate these features, a block-enabled forensic system for IoT, namely the IoT forensic chain (IoTFC) is presented. The proposed system can provide to institutions and examiners the goodness of strong reliability, immutability, traceability, consistency, and dispersed confidence in forensic investigation. The IoTFC guarantees traceability and tracks the origin of the proof. The details of the identification, storage, examination, and presentation of the evidence are recorded in blockchain. The key concept is to retrieve objects from IoT devices and write to blockchain-based IoTFC after examining the connections of each proof item- origin, traceability, and auditability.

Infrastructure-as-a-Service (IaaS) cloud blockchain technology is proposed [40] to solve the problem of centralized evidence collection and preservation. The evidence is collected and preserved in the blockchain in the proposed forensic architecture, which is distributed among multiple peers. Secure Ring Verification based Authentication (SRVA) scheme is proposed for protecting the device from unauthorized users. Secret keys are optimally generated with the use of the Harmony Search Optimization (HSO) algorithm to improve the cloud environment. Based on level of sensitivity and stored in the cloud server, all data is encrypted using the Sensitivity Aware Deep Elliptic Curve Cryptography (SA-DECC) algorithm. Within the SDN controller, a block is generated for each data stored in the cloud and the data history is preserved as metadata. Using Secure Hashing Algorithm-3 (SHA-3), the Merkle hash tree is built into each block. By deploying Fuzzy based Smart Contracts (FCS), the framework allows users to track their data. At last, the analysis of proof is allowed by constructing Logical Proof Graph (LGoE) obtained from the blockchain. Experiments are performed in java (for cloud and blockchain) and network simulator-3.26 (for SDN) optimized environment. The detailed analysis shows that the proposed forensic architecture shows promising results in response time, evidence insertion time, evidence testing time, overhead communication, hash calculation time, key generation time, encryption time, decryption time, and overall change rate.

A greater attention is paid to the protection of logs created during cloud data activity [41]. Although cloud data is compromised and exploited by various security threats (e.g. defective operations, hacker attacks etc.), log analysis is one of the most common methods for monitoring incidents. Maintaining the confidentiality of log files is a requirement for completing the monitoring of the incident. This paper introduces a public model focused on a third-party auditor to check the accuracy of cloud logs. To avoid log data being altered, the log block tags using the classic Merkle hash tree structure are aggregated and the root node that will be stored in the blockchain are created. However, during the public audit, the proposed scheme leaks no log material. The theoretical study and empirical analysis demonstrate that the framework can successfully extend the security audit of cloud logs in terms of the overhead computational complexity, which is better than the past. In particular, the homomorphic hash function to produce log block tags is used. Since the tag is generated by the CSP and the CSP is not completely trusted, Merkle hash tree log tags are aggregated and the tree root is published with blockchain, which not only reduces CSP's computational costs to generate tags but also prevents log tags from being tampered with.

6. Conclusion and Future Works

The technological advancements and the use of excessive internet have given a wider rise to the cloud-based approaches in forensics to investigate the attacks performed on the larger data storage on a cloud. The results of the various studies have represented a contribution of cloud computing in digital forensics. The research work represents the various stages involved in the traditional and cloud based digital forensics. We have identified that cloud forensics is the combination of cloud computing and digital forensics. The implementation of cloud computing in digital forensics is a tedious task. Thus, the study has represented the various IoT based approaches to implement cloud digital forensics. We have focused on three zone- based approach in which first zone deals with the internal network including sensors, wireless devices, and data about the stages. The second zone includes the internal network and third zone include all the public network devices. The studies show that cloud computing in digital forensic provides large data storage, computational capabilities and network security features which help to investigate the malicious activities performed on the cloud. The stages of cloud based forensic process involve various types of challenges and issues on each stage. Thus the various possible challenges and risks on every stage have been evaluated with the proposed solutions to the challenges.

The discussions in the study are mainly focusing on the security challenges and issues when digital forensic integrated with cloud computing. As a future work, these security challenges and issues can be transmitted as solution to design a secure network. Some other ways can be implemented to enhance the security by migrating cloud services. To better understand and resolve the cloud forensic challenges, a comprehensive and real-life scenario can be constructed to cover various aspects. Also, an enhanced featured framework can be developed to support generation of the forensically evidences of sound. The existing frameworks for digital forensics lack the required standards; thus, they are not appropriate for cloud environment. The various attackers always attempt to take advantage and influence the weak areas in the network. Thus, in future a standardized framework should be developed to permit enhanced investigations in digital forensics and can be capable to detect the malicious users who can be punished.

References

[1] 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.

[2] M. Harbawi and A. Varol, “An improved digital evidence acquisition model for the internet of things forensic i: A theoretical framework,” in 2017 5th International Symposium on Digital Forensic and Security(ISDFS). IEEE, 2017, pp. 1–6.

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

[4] S. Simou, C. Kalloniatis, E. Kavakli, and S. Gritzalis, “Cloud forensics: identifying the major issues and challenges,” in International conferenceon advanced information systems engineering. Springer, 2014, pp. 271– 284.

[5] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of things forensics: Challenges and approaches,” in 9th IEEE International Conferenceon Collaborative computing: networking, Applications andWorksharing. IEEE, 2013, pp. 608–615.

[6] J. Dykstra and A. T. Sherman, “Understanding issues in cloud forensics: two hypothetical case studies,” UMBC Computer Science and ElectricalEngineering Department, 2011.

[7] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. Sani, S. Shamsuddin, and F. Norouzizadeh, “A survey about impacts of cloud computing on digital forensics,” International Journal of Cyber-Security and DigitalForensics, vol. 2, no. 2, pp. 77–94, 2013.

[8] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, “A survey on cloud forensics challenges and solutions,” Security and CommunicationNetworks, vol. 9, no. 18, pp. 6285–6314, 2016.

[9] A. K. Mishra, P. Matta, E. S. Pilli, and R. Joshi, “Cloud forensics: Stateof- the-art and research challenges,” in 2012 International Symposium onCloud and Services Computing. IEEE, 2012, pp. 164–170.

[10] C. Liu, A. Singhal and D. Wijesekera, “IDENTIFYING EVIDENCE FOR CLOUD FORENSIC ANALYSIS,” IFIP International Federation for Information Processing, p. 111–130, 2017.

[11] S. O'shaughnessy and A. Keane, “Impact of Cloud Computing on Digital Forensic Investigations,” in 9th International Conference on Digital Forensics (DF), Orlando, FL, 2013.

[12] S. Almulla, Y. Iraqi and A. Jones, “A State-Of-The-Art Review of Cloud Forensics,” Journal of Digital Forensics, Security and Law, vol. 9, no. 4, pp. 6-28, 2014.

[13] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, “A review and comparative study of digital forensic investigation models,” in InternationalConference on Digital Forensics and Cyber Crime. Springer, 2012, pp. 314–327.

[14] E. Fleischet al., “What is the internet of things? an economic perspective,” Economics, Management, and Financial Markets, vol. 5, no. 2, pp. 125–157, 2010.

[15] L. Coetzee and G. Olivrin, “Inclusion through the internet of things,” in Assistive Technologies. IntechOpen, 2012.

[16] J. Gantz and D. Reinsel, “The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east,” IDC iView: IDCAnalyze the future, vol. 2007, no. 2012, pp. 1–16, 2012.

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

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

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

[20] C. Liu, A. Singhal and D. Wijesekera, “Identifying Evidence for Cloud Forensic Analysis”, IFIP International Federation for Information Processing, p. 111-130, 2017.

[21] G. Sibiya, H. Venter and T. Fogwill, “Digital Forensics in the Cloud: The State of the Art”, in IST- Africa 2015 Conference Proceedings, Pretoria, 2015.

[22] D. Jariwala, “Cloud Forensics: What is it? And Why is it Important?”, Techstagram, 20 March, 2013. Available: https://www.techsragram.com/2013/03/20/cloud-forensics-importance/. [Accessed 20 September 2019].

[23] R. Keyun, J. Carthy, T. Kechadi, and M. Crosbie. "Cloud forensics." In *IFIP International Conference on Digital Forensics*, pp. 35-46. Springer, Berlin, Heidelberg, 2011.

[24] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis. "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues." *IEEE Communications Surveys & Tutorials* (2020).

[25] M. Lang, M. Wiesche, and H. Krcmar, “Criteria for selecting cloud service providers: A Delphi study of quality-of-service attributes,” Inf. Manag., vol. 55, no. 6, pp. 746–758, Sep. 2018.

[26] Y. R. Stoyanov, “An approach to use the Web services and open source software to store and share user applications and data,” in Proc. Annu. Univ. Sci. Conf. NVU, vol. 9, pp. 92–96, 2014.

[27] Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasurbramanian, V. A Lightweight Blockchain Based Framework for Underwater IoT. Electronics 2019, 8, 1552.

[28] Uddin, Md Ashraf and Stranieri, Andrew and Gondal, Iqbal and Balasubramanian, Venki, “Blockchain leveraged decentralized IoT eHealth framework”, Internet of Things, Elsevier, v. 9, pp. 100159, 2020.

[29] Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasurbramanian, “A Decentralized Patient Agent Controlled Blockchain for Remote Patient Monitoring”, 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, Spain.

[30] Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasurbramanian, “Blockchain Leveraged Task Migration in Body Area Sensor Networks”, The 25th Asia-Pacific Conference on Communications (APCC), IEEE, Vietnam, 2019.

[31] Sidra Anwar, Sadia Anayat, Sheeza Butt, Saher Butt, Muhammad Saad, " Generation Analysis of Blockchain Technology: Bitcoin and Ethereum", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.12, No.4, pp. 30-39, 2020. DOI: 10.5815/ijieeb.2020.04.04

[32] Mousumi Mitra, Aviroop Chowdhury, " A Modernized Voting System Using Fuzzy Logic and Blockchain Technology", International Journal of Modern Education and Computer Science(IJMECS), Vol.12, No.3, pp. 17-25, 2020.DOI: 10.5815/ijmecs.2020.03.03

[33] Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi, Gary B. Wills, "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions", International Journal of Intelligent Systems and Applications(IJISA), Vol.10, No.6, pp.40-48, 2018. DOI: 10.5815/ijisa.2018.06.05

[34] Hossein Mohammadinejad, Fateme Mohammadhoseini, "Privacy Protection in Smart Cities by a Personal Data Management Protocol in Blockchain", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.3, pp.44-52, 2020. DOI: 10.5815/ijcnis.2020.03.05

[35] Somdip Dey, " A Proof of Work: Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory ", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.8, No.5, pp. 1-9, 2018.DOI: 10.5815/ijwmt.2018.05.01

[36] Al-Khateeb H., Epiphaniou G., Daly H. (2019) Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger. In: Jahankhani H., Kendzierskyj S., Jamal A., Epiphaniou G., Al-Khateeb H. (eds) Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications. Springer, Cham.

[37] Jun Hak Park, Jun Young Park, and Eui Nam Huh, “Block Chain Based Data Logging And Integrity Management System For Cloud Forensics”, International Conference on Computer Science, Engineering and Applications, pp. 149– 159, 2017.

[38] Duc-Phong Le, Huasong Meng, Le Su, Sze Ling Yeo, and Vrizlynn Thing, “BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy”, Proceedings of TENCON 2018 - 2018 IEEE Region 10 Conference, 2018.

[39] Shanking Li, Tao Qin, and Geyong Min, “Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems”, IEEE Transactions On Computational Social Systems, VOL. 6, NO. 6, DECEMBER, 2019.

[40] Mehran Pourvahab, And Gholamhossein Ekbatanifard, “Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology”, Special Section On Emerging Approaches To Cyber Security, IEEE Access, 2019.

[41] Jia Wang, Fang Peng, Hui Tian, Wenqi Chen, and Jing Lu, “Public Auditing of Log Integrity for Cloud Storage Systems via Blockchain”, Springer Nature Switzerland AG, LNICST 284, pp. 378–387, 2019.

Authors’ Profiles

Omi Akter is currently doing her Bachelor’s in Electrical and Electronic Engineering from Chittagong University, Chittagong, Bangladesh. She has published several research papers. She has research interest on communication and computer network, blockchain technology, security and privacy, digital forensics etc.

Arnisha Akhter received her B.Sc. and M.Sc. degree in Computer Science and Engineering from Jagannath University, Dhaka, Bangladesh. She has been working as a faculty member in the same department now. She has published several good research articles in top quality conferences and Journals. Her research interest includes Artificial Intelligence, Data Mining, Wireless Ad Hoc and sensor Networks etc.

Md Ashraf Uddin received his B.S. and M.S. degrees in computer science and engineering from the University of Dhaka. Currently, he is pursuing his Ph.D. at Federation University Australia. he is serving as an Assistant Professor in the Department of Computer Science and Engineering, Jagannath University, Dhaka Bangladesh. His research interests include privacy and security in Remote Patient Monitoring, Blockchain, modelling, analysis, and optimization of protocols and architectures for underwater sensor networks, artificially intelligent, data mining, and so forth.

Dr. Md. Manowarul Islam received his Ph.D from the Department of Electrical and Communication Engineering, Okayama University, Japan in 2019. He received the B.Sc. and M.S. degree in Computer Science and Engineering from the University of Dhaka, Bangladesh in 2010 and 2012 respectively. Currently, he is working as Assistant Professor in the Dept. of Computer Science and Engineering, Jagannath University, Dhaka, Bangladesh. His research interests include Computer Networking, Cloud Computing and Machine Learning.

How to cite this paper: Omi Akter, Arnisha Akther, Md Ashraf Uddin, Md Manowarul Islam, " Cloud Forensics: Challenges and Blockchain Based Solutions", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.10, No.5, pp. 1-12, 2020.DOI: 10.5815/ijwmt.2020.05.01