International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Mar-24)

https://dx.doi.org/10.12785/ijcds/150173

Forensics Analysis of Cloud-Computing Traffics

Moayad Almutairi[1], Shailendra Mishra[2] and Mohammed AlShehri[3]

[1,2,3]*Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah, Saudi Arabia*

Received 28 Apr. 2023, Revised 630 Jan. 2024, Accepted 7 Feb. 2024, Published 1 Mar. 2024

Abstract: The objective of forensic analysis of cloud computing traffic is to identify any suspicious or malicious behavior in network activities within cloud computing settings. This includes examining network connections, data transfer patterns, and data payloads. To effectively analyze cloud computing traffic associated with IoT devices, it is imperative to understand cloud infrastructure and network protocols. The prevalence of IoT devices in cloud environments necessitates efficient forensic analysis techniques to address security incidents. Considering the distinctive attributes of IoT devices and the decentralized nature of cloud environments, this paper investigates the challenges and considerations related to forensic analysis in cloud computing systems incorporating IoT devices. The framework we present includes comprehensive guidelines about data collection, preservation, analysis, and forensic analysis in IoT-based cloud computing systems. As well as providing practical case studies, we demonstrate how our framework works in real-world scenarios involving IoT-based cloud computing. Providing tangible solutions to the forensic challenges specific to IoT-based cloud computing systems, the findings of this research contribute significantly to a better understanding of these challenges.

Keywords: Digital Evidence, Cloud Forensic, Windows 11 Registry, Forensic artifacts, Cybersecurity.

I. Introduction

Cloud forensics, a vital component of digital forensics, involves the meticulous collection, preservation, analysis, and presentation of digital evidence within cloud computing environments. With the ever-growing integration of cloud computing and the Internet of Things (IoT), forensic analysis in IoT-based cloud computing systems presents unique and evolving challenges. This research paper seeks to address these challenges and propose a practical framework for conducting forensic analysis within IoT-based cloud computing systems [1]. Cloud service companies see this as a chance to devise new business models. Unlike traditional computer devices that rely on established network security suites such as secure routers, IoT interaction comprises an infinite variety of channels, impacts, and standards [2]. Cloud technology is a continually evolving technology solution and business, as seen by the growth in the global adoption of the products it provides [3]. Whereas cloud technology has its roots in personal computers, which has some connections to traditional Web-hosting, the way services are delivered dramatically. As organizations increasingly migrate their data and applications to the cloud, the significance of cloud forensics has surged [3]. Cloud computing, bolstered by its widespread adoption, has evolved considerably in recent years [4]. Notably, IoT devices have become an integral part of cloud ecosystems, introducing a new layer of complexity to forensic investigations [5]. Ensuring security and data integrity across all layers of IoT-based cloud computing is paramount to the success of forensic analysis [6]. The analysis of cloud computing IoT (Internet of Things) traffic involves investigating and analyzing network traffic in a cloud computing environment that is associated with IoT devices [7]. This can include identifying and analyzing network connections, identifying and analyzing data transfer patterns, and identifying and analyzing data payloads between IoT devices and the cloud [8]. The method is divided into three categories in cloud computing Client-side, Server-side, and network-side.

Cloud computing refers to the process of conducting forensic investigations on client devices that are connected to cloud services. This can include analyzing data stored on the client device, extracting data from the device's sensors, or examining the device's network activity [9]. One of the main benefits of forensic analysis on the client side in cloud computing is that it allows for a more targeted and efficient investigation. To conduct forensic analysis on the client side in cloud computing, it is important to use appropriate forensic tools and techniques that are designed to work with cloud services. This can include tools for analyzing data stored on the client device, extracting data from the device's sensors, or examining the device's network activity. In addition, it's

E-mail address: 431104384@s.mu.edu.sa, s.mishra@mu.edu.sa, ma.alshehri@mu.edu.sa

important to have a clear understanding of the legal and regulatory requirements that apply to the cloud environment and to ensure that the forensic analysis is conducted in compliance with these requirements. This includes ensuring that the evidence is collected and analyzed in a way that preserves its integrity and admissibility in court. Overall, forensic analysis at the client side in cloud computing can provide a valuable tool for conducting forensic investigations and preserving the integrity of the evidence. However, it is important to be aware of the challenges associated with this approach and to take appropriate measures to mitigate them.

Forensic analysis on the server side of cloud computing typically involves analyzing the cloud infrastructure and the servers that host the data [10]. The process can include identifying the cloud provider and determining the specific cloud service(s) used.

- Collecting data from the cloud infrastructure, such as log files, system configurations, and metadata.
- Examining server virtual machines and the data stored on them, such as file systems, databases, and application data.
- Analyzing the data to identify any signs of malicious activity, such as unauthorized access or data breaches.
- Preserving the evidence in a forensically sound manner, such as creating bit-by-bit copies of the data.
- Presenting the evidence in a way that is legally admissible and understandable to non-technical audiences.

To perform a forensic analysis on cloud servers, it is important to have an in-depth understanding of the cloud provider's infrastructure and the data storage technologies used. The process also involves collaboration with the cloud provider to ensure the preservation of the evidence and compliance with legal and regulatory requirements. It's also important to keep in mind that cloud providers have their policies and procedures for handling digital evidence, so it's important to be familiar with the providers' legal and regulatory requirements before starting the forensic analysis. Forensic analysis on a cloud computing network involves investigating and analyzing data from the network to determine what occurred and who involved in a security incident was. This can include analyzing network traffic, reviewing system and application logs, and examining data stored in the cloud. Cloud service providers need to have a plan in place for forensic analysis in the event of a security incident, as well as to work with a qualified forensic investigator who is familiar with cloud computing technologies. The aim of forensic analysis of cloud-computing traffic on IoT (Internet of Things) is to analyze and extract information from network traffic to identify and investigate potential security breaches, malicious activity, or other incidents on IoT devices connected to cloud services [10].

The objectives of this study include:

- Identifying and extracting relevant data.
- Network traffic.
- Investigating incidents.
- Preservation of evidence.
- Compliance with legal and regulatory requirements.

The purpose of this research is an inquiry to find answers. With the growing need for harnessing the Cloud's ability to process sensitive files and data. It reveals who developed and who updated certain types of data in the Cloud. As to physical forensics, there is no one technique to determine how a technology was hacked. These are critical elements for forensic forensics in dispersed systems like the Cloud. This study attempts to give helpful information to Forensic analysis investigators who collect evidence from Cloud-based IoT devices. Because it is challenging to create frameworks and rules that will work in all situations, more testing and study can give the knowledge to enhance current practices. The paper's goal is for the results to help the future development of efficient forensic processes in the Cloud-IoT environment.

To achieve the paper's objectives, it is divided into six sections. The first section introduces the topic, while Section 2 examines related work in cloud forensics. A description of the research methodology and data collection process is provided in section 3. In section 4, the implementation of the study is presented, In section 5 the study's results, implications, and limitations are discussed. Finally, the conclusion, recommendations, and future research directions based on the findings of the study are discussed in section 6.

II. literature Reviews

Cloud forensic, investigation needs to be conducted on both ends client end as well as the server end with confidence that traces of used services will remain in the client machine due to user activities, which holds equal worth in terms of evidence collection during a cyber-incident. In several studies made by many academicians within the client side, they have succeeded in achieving success as compared to the distributed nature of cloud computing where conducting a cloud forensic is a quite tedious job. To finish the inquiry, many methodologies and instruments have been developed. There is a technique of digital forensic evidence in the investigation process so that evidence is obtained, analyzed, and preserved so that the evidence is admissible in court, and integrity and commitment to digital evidence must be adhered to, although there are barriers in the cloud computing environment. Because of its multi-tenancy, attackers use the digital cloud to successfully carry out their attacks, and to solve all crimes related to the cloud environment, a branch of digital forensics known as ”Cloud Forensics” has been introduced, through which cloud forensics can be conducted in the cloud computing environment using digital forensics technology. Cloud service providers are making significant attempts to address concerns such as jurisdiction, dependency on CSP, and tenancy pluralism to prevent cloud system assaults.

According to the National Institute of Standards and Technological (NIST) [11], Microsoft invented PhotoDNA, a forensic science in cloud computing that utilizes scientific concepts, derived methodology, and established technology practices to recreate the past. Cloud computing events that identify, gather, preserve, and analyze evidence for interpretation and reporting. Because cloud forensics involves several deployment strategies and services, the primary challenge is to locate evidence. Because the data is scattered all across the world, there is no way to take any physical device to acquire proof [12]. Cloud computing technology is quite sophisticated, and there is an urgent need to design and innovate technologies that can aid in enhancing cloud computing forensic procedures. Because the service provider has signed contracts with other parties to provide a service to users, the investigator must guarantee that evidence is kept and not tampered with by any third party to produce evidence in court. The chain of custody is the most critical for presenting digital evidence in court; the failure of one of the chains of custody can result in significant damages. If a forensic process is necessary in court under the public cloud model, the investigator cannot confiscate any physical equipment, as in the case of a building fire. It employs a private internal cloud model that allows forensic processes to be performed in the same manner as traditional forensic procedures; however, if the business employs an external cloud model, but privately, the investigator must rely on it to gather data or log files [13].

After the advent of cloud computing technology, many new sorts of services were available, allowing users to access various types of services over the network. In terms of user accessibility, there are three categories of services: infrastructure, software, and platform. Public, private, communal, and hybrid distribution models are used. Users of mobile devices and laptops utilize cloud services to keep their data in it, and their data is saved in different servers all over the world [14]. Because data is stored and accessible through the network, many attackers may hack the data. To find attackers or reduce crime, (NIST, 2014b) defines ”Cloud Forensic Science” as ”the application of scientific principles, technological practices, and derived and proven methods to replay previous cloud computing events by identifying, collecting, archiving, examining, and reporting digital evidence”.

Scholars [15] have suggested several approaches in cloud forensics during the last 12 years. This section discusses the framework and techniques in detail. In [16] authors give a complete review of the cloud forensics particular survey. The paper also presents a cloud forensics taxonomy based on cloud computing paradigms influencing cloud forensics. Whereas forensics remedy taxonomy was offered previously, this work seeks a more generalized taxonomy solution. The suggested taxonomy provides cloud forensics remedy strategies for practical cloud forensics. The cloud is shifting over time. Cloud improvements will undoubtedly introduce new risks. This is primarily due to increasing domain expertise and growing cloud use in the IT industry. Cloud forensics has problems at every stage of the investigation. The paper’s detailed literature review demonstrates the development of cloud forensics approaching evidence authenticity via blockchain. The paper also highlights the three cloud dimensions that influence the forensics procedure. Throughout this study, we suggest a comprehensive cloud forensic taxonomy that considers obstacles, evidence collecting logistically, interpretation, trust, and legal ramifications. Their future project will focus on developing a mechanism for evidence collecting relying on our suggested typology. They also compared the current frameworks using the suggested taxonomy as measurements. According to the authors, competent evidence collecting and semi-automated evidence processing can help successful cloud forensics. Although trust difficulties cannot be eliminated, an authenticity system can offer the necessary confidence element for the inquiry In [16], authors describe a method for detecting ransomware on an enterprise’s private cloud. After the execution of benign and malicious samples, it captures the volatile memory state of virtual machines and extracts a valuable collection of RAM, file systems, and network properties. The retrieved features are then subjected to feature selection machine learning algorithms to determine the usefulness of the proposed features. Four extensive studies have tested the suggested approach, and the findings show that it can distinguish between benign and ransomware samples. In all experiment configurations, the Random Forest classifier outperformed all other classifiers. The proposed technology may be used to identify infection in virtual business machines successfully.

In [17], some current log-based cloud forensic approaches have been extensively investigated. A complete comparison of the various approaches' benefits and drawbacks has been performed. Research direction opportunities have been discovered by analyzing the limits and benefits of present methodologies.

In [18], the authors discussed the impact of DoS on the server service Cloud Hosting Computing. The Pattern Forensics technique was employed to perform this investigation (The Forensic Process Model). The study's findings will yield digital evidence, such as IP addresses, packet data, and time stamps, indicating the incidence of DoS. Based on the findings of the study and testing conducted using the Forensic Process Model Method, the following conclusions may be drawn: The occurrence of a DoS assault is identified by a surge in traffic, which disrupts the usability or availability of the network service that leads to the Private Cloud Computing service.

In [19], the author discusses the foundations of Cloud Computing & and Vm. The many cloud computing deployment methods and their relationships with user responsibility are being explored. The principles of digital crime prosecution are analyzed through Cloud Computing, and the most critical problems to corruption probes and forensic sciences in this kind and digital environment are provided. The ramifications of cloud computing visualized in criminal probes and crime analysis are examined. The archetypal instance of Nested Virtualization technology is portrayed as a stumbling block to criminal and forensic inquiry. In conventional criminal investigations, it is standard procedure for computer experts to turn off the equipment and create a duplicate of the discs that will be analyzed later in the inquiry. Due to the vast storage capacity, legal difficulties, global dispersion, and data control which may change based on the type of service leased, this is impossible in a cloud computing environment.

environment. Furthermore, the lack of physical access to data collecting and system management makes information acquisition difficult for cloud experts. As a result, forensic computing has been reformed, introducing new approaches, solutions, and research methodologies, giving rise to cloud forensics or cloud expertise. As a result, the Forensic as a Service (FaaS) model is committed to addressing the security concerns inherent in the cloud environment. In this paper, we will look at some of these issues. In [6] analyze the seized digital devices from a murder scene, such as android smartphones, laptops, smartwatches, and so on, to acquire insight into the enemies' illicit actions. They may also recover the data that the enemies have captured or conveyed. Because current gadgets use cloud computing services, cloud analysis is inevitably required in case of a crime scene inquiry. IoT forensics is multidisciplinary since the data to be studied may be acquired from sensors, smart devices, and other devices connected to a crime scene and the cloud. When compared to Cloud Forensics, Digital Forensics is a more straightforward undertaking to do.

Due to distributed and multi-tenant cloud computing, the segregation and collecting of material in a cloud forensic examination is a massive effort. Therefore, there is no similar issue with a digital forensic inquiry. This paper evaluated the scientific community's work on Digital, Hybrid, and IoT Forensics. They contrasted respective efforts or the results of their work and described the current state of the art in Digital, Cloud, and IoT Forensics.

In this [4], the authors recognize and explain the critical concerns involved in the complicated process of IoT-based investigations, namely the ethical, security, and cloud security cases. This paper also overviews prior contemporary theoretical models in digital forensics research. Frameworks that attempt to extract data in a privacy-preserving way or protect evidence integrity utilizing decentralized blockchain-based technologies are given special consideration. Also, the authors discuss the current FaaS prototype and several attractive cross-cutting data reduction and forensics intelligence methodologies. Ultimately, numerous other research trends and unresolved challenges are discussed, emphasizing the need for proactive forensic readiness methods with widely accepted standards. Challenge based on this study and offered security solutions that should address the main components of the issue. Cloud computing is a rapidly growing area of study that depends on sharing processing power rather than employing individual computers or intelligent devices. The universality of electronic and digital devices, as well as the move from a classic IT subscription system to a distinctive cloud model, are responsible for the majority of the growth in this industry. Cloud computing poses a substantial risk and challenge for information system development. It has also been observed that cloud clients and users lack the forensic abilities to detect unlawful activities in the cloud. Even though the cloud provides significant technological and economic benefits, individuals have been hesitant to use it, mainly owing to security problems or the difficulties of completing appropriate cloud research.

Some research [20] has been conducted in this area, as forensic investigative methodologies have been presented. In this study article, they begin by examining other schoolsars' accomplishments in intrusion detection. Still, they look into and assess our findings to determine the potential obstacles cloud forensics confront based on these discoveries.

There have been several research papers published on the use of cloud computing for forensic analysis of IoT traffic. Cloud-based storage and analysis of IoT data can provide increased scalability, storage capacity, and computing power compared to traditional on premise solutions. The use of cloud computing can improve the accuracy and efficiency of forensic investigations by providing access to larger datasets and advanced analytical tools. Research [21] has also explored the use of cloud-based machine-learning techniques for the automated detection and classification of malicious IoT traffic. Some studies [22][23] have also investigated the security and privacy concerns associated with the use of cloud computing for forensic analysis of IoT data, including the need for secure data transmission and storage, and the protection of sensitive formation. Other research [24] has focused on the development of frameworks and tools for the efficient and effective management and analysis of IoT data in cloud environments. These studies highlight the potential benefits and challenges of using cloud computing for forensic analysis of IoT traffic and provide valuable insights for the development of effective and secure cloud-based solutions for IoT forensics [24].

III. Research Methodology

The methodology employed in this research follows a comprehensive and state-of-the-art approach to address the forensic analysis of cloud-computing traffic in IoT-based cloud-computing systems. The methodology consists of the following key steps;

(A) *System design*

Designing a system for forensics analysis of traffic in IoT involves several components, including data collection, data storage, analysis, and reporting. Here's an overview of the high-level architecture for such a system (Figure 1).

Data Collection: The first step is to capture network traffic data from IoT devices and cloud services. This can be done using network taps, port mirroring, or software agents installed on IoT devices. The data collected may include metadata such as timestamps, IP addresses, and protocols used.

Data Storage: The captured traffic data needs to be stored securely for analysis. One option is to store the data in a distributed file system like Hadoop, which allows for scalable and fault-tolerant storage. Alternatively, a NoSQL database like Cassandra can be used for faster query response times. Encryption should be used to secure the data at rest.

Data Analysis: The next step is to analyze the stored data to identify potential security threats or anomalies. This can involve applying machine learn- ing algorithms to detect patterns and anomalies in the data. Additionally, forensic tools can be used to analyze specific data types such as email messages, files, or web browsing history.

Reporting: The results of the data analysis should be presented in a format that is easily digestible for security analysts. This can involve creating dashboards that display real-time threat alerts and visualizations that summarize trends and patterns over time.

Integration: Finally, the forensics analysis system should be integrated with other security tools and processes to ensure that threats are identified and remediated quickly. This can include integration with incident response processes, security information, event management (SIEM) systems, and threat intelligence platforms.

The system design for forensic analysis of IoT in cloud computing typically involves several steps, Which are mentioned below figure.

By adopting this state-of-the-art methodology, the research aims to provide valuable insights into the forensic analysis of cloud-computing traffic in IoT-based cloud-computing systems, contributing to the advancement of the field and enabling forensic investigators to effectively address the challenges posed by these complex environments.

IV. Implementation

(A) *Tools and technique*

In this section, discuss the tools used in this investigation. Instead of going into detail on each device, we've concentrated on the most relevant ones.

1) Tizen Studio:
The official IDE, builds online and native Tizen programs. Developers use Tizen Studio to create Tizen native and web apps. It comes with an integrated development environment (IDE), an emulator, a toolchain, code samples, and a document repository. Smart Development Bridge is a cmd that connects with either a connected target fitness band and has the charge of maintaining connections to the victim machine. The SDB manages several connections to the client machines. The SDB assigns a unique serial number to each connected device, which you may use to give orders to any of those devices. The SDB provides file transfer, remote command, debugger port forwarding, log viewing, and filters, including monitoring for app development.

2) Virtual machine:

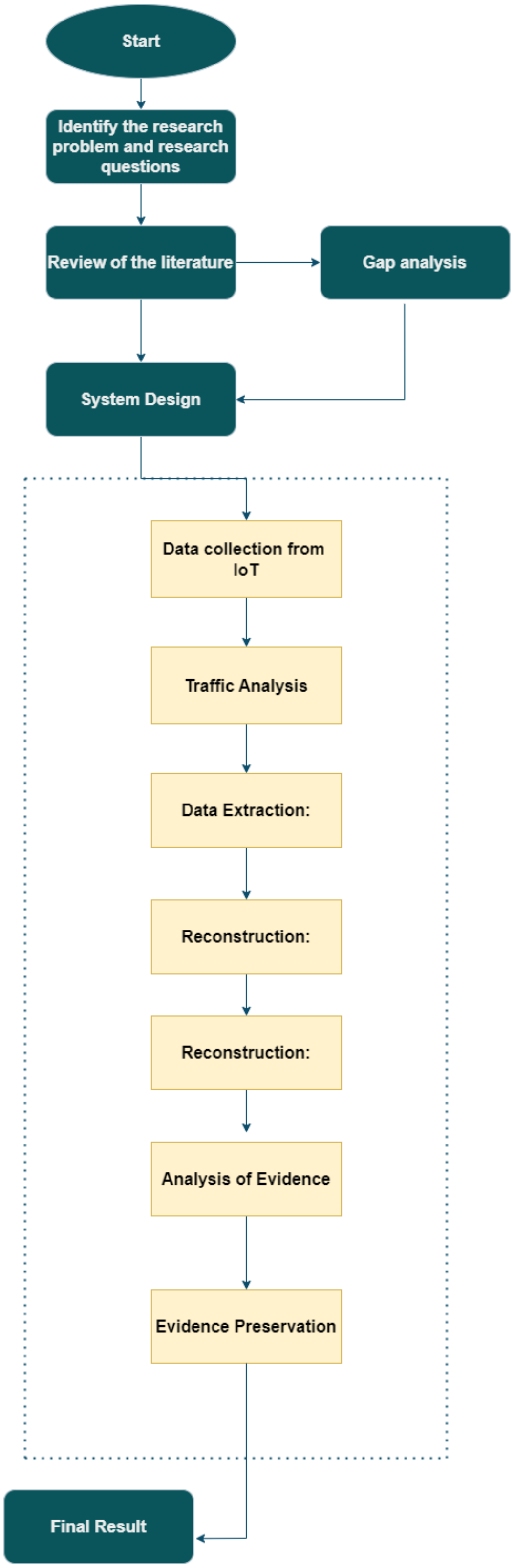


Figure 1. System design

A considerable proportion of solutions for hardware and software are being released in response to the advent of new technologies and research methodologies. The actual device on whose VMS runs is referred to as the Host, while the VMS is referred to as the Guest. A single host may accommodate a large number of visitors [25]. In this phase, run the Gear Gadget code to retrieve the OS built on the Linux kernel from our Smartwatch.

3) Autopsy:
An autopsy is a fully accessible application for forensic procedures on evidentiary disc images. The results of the forensic examination on the disc image are presented below. The information acquired here can be used to explore and discover pertinent information. This technology is used by police agencies, local police, and corporations to analyze evidence uncovered in a cybercrime. It can also be used to recover info that has been deleted.

(B) *Forensic setup for Smartwatch S3*

To facilitate communication between the wristwatch and the laptop, you must disable Bluetooth, activate Wi-Fi, activate the diagnostic option on the smartwatch, or attach it to a WAP generated as a Windows Mobile Hotspot network. Steps to turn off Bluet tooth:
Step 1: Select the turn-off option.
Step 2: To enable developer mode, navigate to options Gear info about the Watch and then software.
Step 3: Next, click the version 5 times.
Step 4: A programmer option switched on start popping up will appear after tapping on the program version.
Step 5: Double-check that the developer mode is displayed in the watch's primary menus.
Step 6: Restart the watch to allow it to initialize.
Step 7: Next, just on Laptop, enable the mobile hotspot settings.
Step 8 After turning on the S3, attach it to WAP. To log in, go to the smart watch's wifi options. Go to Settings Connections Wi-Fi and enable Wi-Fi.
Step 9: The connections will be created and shown in the Laptop Cellular Modem area after tapping on the check. Remember that the IP address will change each time you connect; however, the smartwatch device identifier will remain the same.

(C) *Tizen Studio Setup*

To check yet if the connectivity is formed will require SDB. To do so, 'Install the Tizen studio' set up a link with Smartwatch S3.
Step 1: Now launch Tizen Studio and connect to your

smartwatch S3. Navigate to Tools, Device Manager.
Step 2: Next, touch on the right-hand corner center arrow, which will display information about all intelligent devices.
Click Add after entering the device model IP address from the Mobile Hotspot section.
Step 3: Give the watch name and IP address, and the port will be the same.
Step 4: Following inputting the watch credentials, a pop-up will appear on the watch asking for authorization for SDB interaction with Tizen Studio.
Step 5: The connectivity has been made, so S3 is visible in the device manager. In the area, we can also observe the log events or the Android file system.

(D) *VM setup*

Now have a working seamless connectivity with S3 and Laptop. Then we will set up our environment to obtain the folder of our watch. To do this, one must install Oracle VirtualBox on our PC and create a VM in Oracle VirtualBox.

Step 1: Open VM.
Step 2: Type the name of the VM in my case it is (gears3) and select Type Linux operating system. Version Ubuntu (64 bit), memory size 5 GB Ap- proximately and use existing image name (GearGad- get:dsk1.vmdk.
Step 3: Our virtual machine is now established. Place the image gears3 in the upper left corner and choose Style.
Give the username and password. Now the VM is launched. Open terminal in Vm Setting up custom Inbound outbound rule in watch S3.

To link the Virtual Machines, we must first build incoming and outbound rules.

Open Control Panel System and Security Windows Defender Firewall and click Advanced Settings in the left pane to configure inbound rules.

1) *Click New Rule in the left pane and then proceed with the Program checkbox selected.*
2) *Next, choose the usual All Programs option.*
3) Review the Allow connection box.
4) *Check domain public and private.*
5) *Name the rule GearS3.*
6) *Check GearS3 power created in inbound.*
7) *Observe the exact measures for the outbound rule, also.*
8) *Click the outbound area, from the left pane, and click Create a rule.*
9) *Network Configuration for a VMs.*
10) *Configure the VMS so that the VM can connect with the Gear Gadget.*
11) *Right-click the VM and go to its settings.*
12) *Within Configuration, navigate to the network segment, choose the Bridged adapter, uncheck the Cable connected box, and set the Promiscuous mode to ”Allow All” before pressing OK.*

(E) *GearGadget S3 Connection*

1) *Enable the Mobile Hotspot Window to view the watch information.*
2) *Type IP configuration to display the device IP, 192.168.0.99, under Wireless LAN adapter WI-FI; ping this IP from the Virtual Machine to ensure that the machines can connect. (Please keep in mind that your IP address will be different. Take note of the IP address 192.168.137.1 under Wireless LAN adapter Local Area Connection.*
3) *This is the Internet Protocol address assigned to devices connecting to the Windows hotspot. We linked our watch to this network and obtained the IP address 192.168.137.57. More on that later.*
4) *Likewise, in VMS, input the IP config and ping the VM machine's IP address from Window frames.*
5) *Ping the Vm at 192.168.137.1.*
6) *This will tell us how we can interact with both the device that is attached to the hotspot.*
7) *Another critical thing to remember is that the ping command should run continuously with live replies throughout the procedure. In any event, if replies cease arriving at the VMS, re-establish the request packet with practical contribution, acquisition will be impossible.*

   Furthermore, it would help if you kept an eye on the ping terminal window to see whether there are any answers to ping queries.

(F) *Running Script bash.GearGadget.sh*

Try Ping Obtain admin rights on your virtual computer through the sudo su function, then input passcode forensics, as shown in the script. GearGadget.sh needs root privileges to execute. Furthermore, 2 major facts to remember from the Mobile Hotspot Pane are the Devices Name and the Destination IP.

(G) *Enter command in terminal* Another issue seen in the above screenshot is that many of the files shown as authorization refused are because the Gear Gadget phone is not rooted, requiring additional detail at the root level, which is not always necessary but relies on the goal of forensics. A message will pop up in the interface after completing the filesystem extraction. Before the first, if you see no output at any point, don't rush; instead, wait. Next, repeat the acquisition procedure at least twice because our relationship with the device might drop and the extracting still needs to be completed. Thus, obtaining data twice and checking its magnitude would give us confidence in the Watch's fault-less collection.

In the above image are the acquired files, including logs, MD5 hash, and opt directory, which is our main extraction/acquisition to analyses. Discover the MD5 hash of the obtained data in the GearS3 Different extraction directory, allowing us to do an integrity check. Above, see a recovery of approximately 190 MB that can be analyzed manually or using forensics software. The data collected using the GearGadget utility is saved in the current directory. The folder may then be examined using any forensics software.

V. Forensic Analysis

(A) *GearS3 Image Forensic Analysis*

The purpose of the research was to see whether it was possible to locate data supporting an examination. E extracted data and saved them as photos on the Gear S3 using the Tizen operating system's file system. After we completed uploading the data, we moved on to the next phase, which involved utilizing the analytical program Autopsy. The following section will offer a step-by-step explanation with supporting graphics for the forensic expert's virtual folders and files and the material that might be discovered within them. The data will be presented in tabular form.

(B) *Extracted/Acquired Image Forensics*

This data, approximately 190 MB in size, may be extracted manually or using forensics tools. The data itself is around 190 MB in size. The work done by capturing data with the help of the GearGadget script may be located in the recipient's root folder. Following that, a scientific investigation into that folder will be conducted using the Autopsy software, which is consistent and much more efficient in the environment.

(C) *Procedure for Smart Watch Forensics Using an Autopsy*

Using an Autopsy To begin, launch the Autopsy investigations program. An autopsy will launch a window with the options to initiate a new case, open a Recent case, or start a case. We'll start with Create New Case.

Once a new case is, provide the case name and specify the directory for which an autopsy will preserve case data, as shown below. Following that, click 'Next' to go to the next phase.

- An autopsy will now request case-specific material such as a case number, Examiner name, Examiner phone number, and so on. To finish the case initialization stage, click 'Finish.'
- After pressing the 'Finish' option, Autopsy will display the window below.

Now finished the case initialization process, in which we were requested for case-related info. Secondly, we'll enter the data source we wish to examine during the autopsy. Autopsy supports a wide range of data source formats. Also, have a Smartwatch file type with picture data in the 'opt' folder. That opt folder will need to be added as a Source Of data. As a result, we will pick 'Logical File' and then click 'Next' to proceed.

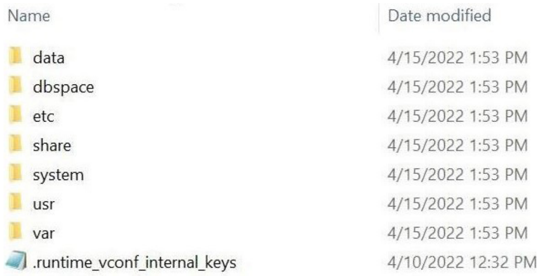
- *Following choosing 'Next,' add a folder to investigate by choosing the 'Add' button. To continue, click the 'Next' button.*
- *An autopsy will open a window that will ask the examiner what kind of data he is looking for.*
- *Click on 'Select All' to mark the entire set of data to be examined. Click 'Next' to proceed further.*
- *Press the Next and Finish buttons.*
- *Inserted source data successfully. Now, look at the data that was taken from that source.*
- *Let's look at the different portions of autopsy windows and their functions.*
- *The leftmost pane has a Data Sources hierarchy. Extracted data is classified into many types, and each category is presented on this page.*
- *The files in the upper right pane are within a*

folder/data source. The Data Source, for example, comprises one file, "LogicalFileSet1," as seen in the upper right pane below.

- *The data from the upper right window is shown in the lower right pane.*
- *The file data for "LogicalFileSet1" is presented in the lower right pane, as illustrated below.*

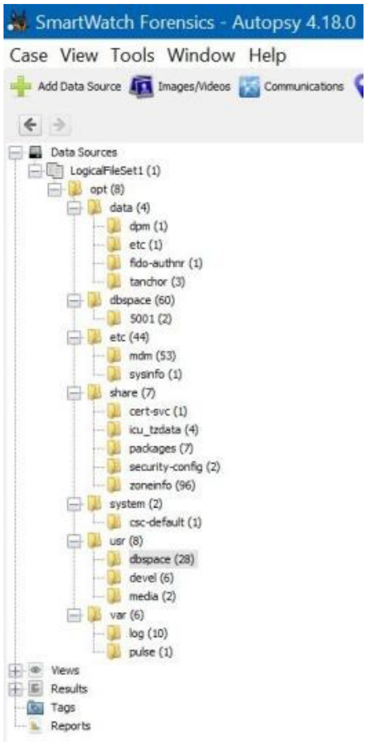
(D) *Views*

Data was organized into three categories by Autopsy. A Smartwatch file system is similar to an Android file system in that picture data is stored in a hierarchical structure within an opt folder It divides data into 3 subcategories. In Figures 2, 3,4, 5 and 6 show data source, data lode, categoriess, Check MME, and results are shown in Figure 7.



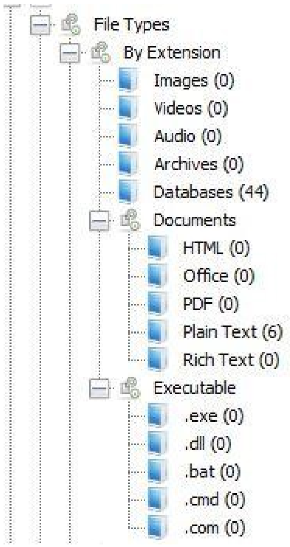
Name	Date modified
data	4/15/2022 1:53 PM
dbspace	4/15/2022 1:53 PM
etc	4/15/2022 1:53 PM
share	4/15/2022 1:53 PM
system	4/15/2022 1:53 PM
usr	4/15/2022 1:53 PM
var	4/15/2022 1:53 PM
.runtime_vconf_internal_keys	4/10/2022 12:32 PM

Figure 2. Data Source


SmartWatch Forensics - Autopsy 4.18.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications

```
Data Sources
  LogicalFileSet1 (1)
    opt (8)
      data (4)
        dpm (1)
        etc (1)
        fido-authnr (1)
        tanchor (3)
      dbspace (60)
        5001 (2)
      etc (44)
        mdm (53)
        sysinfo (1)
      share (7)
        cert-svc (1)
        icu_tzdata (4)
        packages (7)
        security-config (2)
        zoneinfo (96)
      system (2)
        csc-default (1)
      usr (8)
        dbspace (28)
        devel (6)
        media (2)
      var (6)
        log (10)
        pulse (1)
Views
Results
Tags
Reports
```

Figure 3. Data Load



```
File Types
  By Extension
    Images (0)
    Videos (0)
    Audio (0)
    Archives (0)
    Databases (44)
    Documents
      HTML (0)
      Office (0)
      PDF (0)
      Plain Text (6)
      Rich Text (0)
    Executable
      .exe (0)
      .dll (0)
      .bat (0)
      .cmd (0)
      .com (0)
```

Figure 4. Categoriess

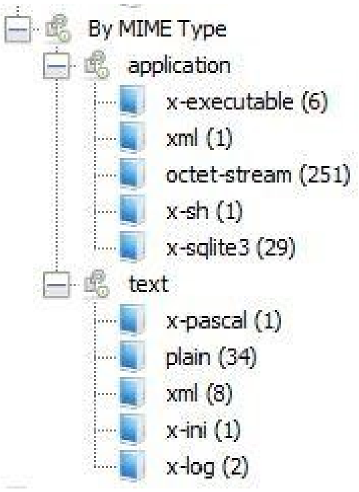


Figure 5. Check MME

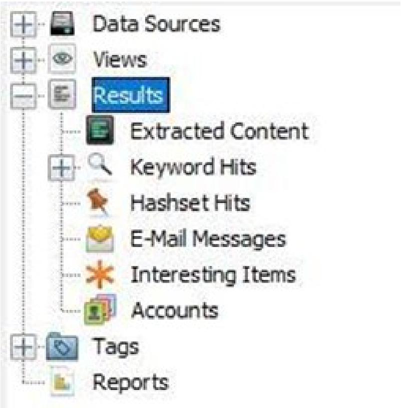
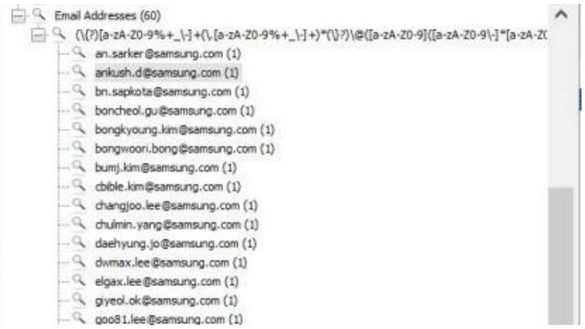


Figure 6. Check result section

The "Keyword Hits" section in a forensic analysis report would typically contain the results of a keyword search conducted using a tool such as Autopsy (Figure 6). The Autopsy default search script is designed to search through a given set of data, such as a computer's hard drive or memory, and identify specific keywords or phrases. In this case, the script has returned a result of 60 email addresses that were found within the data set (Figure 7). These email addresses may be relevant to the investigation and could be used as a lead for further analysis. It is important to note that the context of the investigation is not provided, so I cannot give more specific details about what the email addresses may be related to. However, the forensic analyst should document the results of the search in the report, including the keywords or phrases used in the search, the number of hits found, and any relevant information about the hits (e.g. email addresses, file names, etc.).



```
Email Addresses (60)
  (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z(
    an.sarker@samsung.com (1)
    ankush.d@samsung.com (1)
    bn.sapkota@samsung.com (1)
    boncheol.gu@samsung.com (1)
    bongkyoung.kim@samsung.com (1)
    bongwoori.bong@samsung.com (1)
    bumj.kim@samsung.com (1)
    cbible.kim@samsung.com (1)
    changjoo.lee@samsung.com (1)
    chulmin.yang@samsung.com (1)
    daehyung.jo@samsung.com (1)
    dwmax.lee@samsung.com (1)
    elgax.lee@samsung.com (1)
    giyeol.ok@samsung.com (1)
    goo81.lee@samsung.com (1)
```

Figure 7. Email Address

In a forensic analysis report, the list of all emails within a specific search category would typically be presented in a tabular or bullet point format, with each email address listed on its own line. The list would be accompanied by a description of the search category.

An example of how the email addresses might be presented in the report is shown below:

Email Addresses found in the ".pkgmgrparser.db" database. In this research, the email address "ankush.d@samsung.com" was found from the ".pkgmgrparser.db" database as highlighted in the lower right window. This information is also highlighted in the report to indicate the specific location of the email address within the data set, it can also be used for the purpose of further analysis and investigation. It is important to note that the context of the investigation is not provided, so I cannot give more specific details about what the email addresses may be related to. However, the forensic analyst should document the results of the search in the report, including the keywords or phrases used in the search, the number of hits found, and any relevant information about the hits (e.g. email addresses, file names, etc.)

(E) E. Analysis of Extracted Data

During a forensics investigation, it is common to use various tools and techniques to extract useful information from different types of data sources, such as a smartwatch image file. A smartwatch image file can contain a wealth of information, such as time and date stamps, GPS coordinates, and other metadata that can be used to help establish a timeline of events or to identify suspects or victims. In a forensic analysis report, the information obtained from a smartwatch image file would typically be presented in a clear and concise manner, including:

- Description of the image file, including the make and model of the smartwatch and the method used to acquire the image.

- Summary of the information found in the image file, such as time and date stamps, GPS coordinates, and other relevant metadata.
- Screenshots or images of the data found in the image file to help illustrate the information found.

It is important to note that the context of the investigation is not provided, so I cannot give more specific details about what the smartwatch image file may contain, but it could be used to establish the timeline of events, identify suspects or victims, and gather other useful information related to the investigation.

It is also important to note that the information obtained from the smartwatch image file should be verified and validated, and any assumptions made during the investigation should be clearly documented and explained in the report.

Tizen is an operating system developed by Samsung for use on a variety of devices including smartphones, smart TVs, and smartwatches. It's an open-source platform based on Linux and is designed to be compatible with a wide range of devices.

The Tizen advertising identifier is a unique identifier that is used to track a user's activity on Tizen-powered devices for advertising purposes. It allows advertisers to deliver targeted advertisements to users based on their preferences and browsing history.

The volume popup that you mentioned is likely a feature built into the Tizen operating system that alerts the user when they adjust the volume on their device.

It is important to note that some users may find the collection and use of these advertising identifiers to be a privacy concern. In most cases, users have the option to opt-out of targeted advertising by disabling the use of these identifiers in their device settings.

The ".clock list order.db" file is likely a database file that contains information about different clock configurations on a Tizen device. The data contained within the file likely includes information about different clocks, such as their view (analog, digital, or hybrid), their configuration settings, and any other relevant information. It is possible that this file is used by the device's clock application to store and retrieve the user's clock preferences and settings, such as the order in which the clocks are displayed, the clock faces that are used, and any other customization options. It is important to note that this file may contain sensitive information such as timezone and alarms, and it's important to handle this data with care during forensic investigations.

I discovered the "critical-log.log" file while manually analyzing the picture file. This file provides a log of various events, such as power off, boot, and traction battery, as well as the time window for each occurrence.

VI. Results & discussion

The findings are designed to represent the analysis's actual essence; it is helpful to evaluate whether all technical forensic procedures are what they claim to be; this will be a simple method of identifying essential files. Os uses application binding to attach a file system to an application. Interface, for example, uses file extensions and keeps track of which applications may open specific files. To open doc files, use Microsoft Word. Although Windows uses file extensions, there is a data-hiding method in which a user may change the extension of a document to conceal its content. On the Samsung Gear S3, the results show that tools surpass open-source applications in cloud computing environments. To use these technologies necessitates fundamental knowledge for an implementation to be carried out. The study is strongly reliant on timely data collecting. Samsung hardware has a limited attention span and frequently overwrites previous data. After getting a watch for forensic analysis, the first step should be to put it in airplane mode, not use it, and turn it off. As a result, it is possible to ensure that no outside data mutation happens in the timeline of the file as mentioned above analyses. The statistics depict the duration of the occasion and the event. Following the production of events.

Hand motion, wrist rotation, and band swiping of a person wearing it were all recorded. This data may be utilized to determine the exact time of watch usage various watch statuses, such as accept or refuse, are also recorded. The database of the "MapMyRun" application exposes heart rate data when in an active exercise state. Using the "Survey-Log.DB," it is difficult to detect signals from the Samsung Health application about behavior or mobility. GPS and LBS data do not give detailed information about the watch's location. The watch's position may be estimated using data from air pressure sensors, temperature, and sea level air pressure.

Discussion

Confidential organizations and governmental departments fulfill security quality measure criteria in technologies such as the Samsung Gear S3. Several specific programs or interactions with the system and forensic testing activities are anticipated to ensure correct implementation and comprehension via study. The Federal Bureau of Investigation (FBI), the Defense Department Against Cyber Crime, and other organizations support this policy. Unfortunately, various difficulties develop throughout the technique and tool application while taking any action. This relevance is addressed more below.

A. Challenges faced in Samsung gear using forensic tools:

Forensic analysis of Samsung Gear devices, such as the Samsung Gear S3 and Galaxy Watch, can present a number of challenges due to the device's unique hard-ware and software. Some of the challenges that may be encountered include:

1) **Limited storage:** Samsung Gear devices have limited storage capacity, which can make it difficult to acquire a full forensic image of the device.
2) **Encryption:** Some Samsung Gear devices may be encrypted, which can make it difficult to access the data stored on the device.
3) **Proprietary file system:** Samsung Gear devices use a proprietary file system, which can make it difficult to extract and analyze data using standard forensic tools.
4) **Limited access to the device:** Forensic analysis of Samsung Gear devices may be limited due to the device's small form factor and lack of physical buttons or ports.
5) **Lack of third-party forensic tools:** There is a lack of third-party forensic tools designed specifically for Samsung Gear devices, which can make it difficult to extract and analyze data from the device.
6) **Firmware updates:** The device firmware may be updated frequently and this may cause difficulties in analyzing the device with older versions of forensic tools.

Overall, conducting a forensic analysis of a Samsung Gear device can be challenging, and may require specialized knowledge and tools. It's always recommended to use the latest version of forensic tools available and keep them updated.

B. The use of cloud computing to alter the forensic environment of crime:

1) **Increased storage capacity:** Cloud computing provides virtually unlimited storage capacity, which allows forensic investigators to store and analyze large amounts of data.
2) **Remote access:** Cloud computing allows forensic investigators to access and analyze data remotely, which can be useful for investigations that involve multiple locations or agencies.
3) **Increased collaboration:** Cloud computing makes it easier for forensic investigators to share and collaborate on data and evidence, which can help to speed up investigations and improve their accuracy.
4) **Improved scalability:** Cloud computing allows forensic investigators to scale their computing resources up or down as needed, which can be useful for dealing with sudden spikes in demand or large-scale investigations.
5) **Advancement in forensic tools:** Cloud-based forensic tools are becoming more common, which allow forensic investigators to analyze data in real-time, and access sophisticated algorithms and big data analytics that can help to identify patterns and connections in large data sets.
6) **Cost-effective:** Cloud computing can be more cost-effective than traditional on-premises forensic solutions, as it eliminates the need for expensive hardware and maintenance costs.

However, cloud computing also presents new challenges for forensic investigations, such as security risks, data privacy, and jurisdiction issues. Forensic investigators need to take into consideration the legal and technical requirements of cloud-based evidence and use the appropriate tools and techniques to ensure the integrity and admissibility of the evidence.

Some gadgets, including the Gear S3 or other digital evidence. However, the hard drive of the perpetrators' PCs, tablets, external mobile phones, smartwatches, and other devices would be the principal source of evidence. Because the amount of digital information and storehouse masses differs from person to person, there may be vast quantities of data to analyze time-consuming, and the examination and examination of these can be highly time-consuming, mainly if there is no clear objective in the case that is connected to proper usage.

C. Use of forensic tools for evidence handling

As stated in the study, there is another area for improvement with most digital gadgets. There is evidence of uncertainty in the handling procedure. Proper evidence handling is a critical aspect of forensic tool usage to ensure the integrity and admissibility of the evidence in a court of law. Some key considerations for evidence handling when using forensic tools include:

1) Chain of custody: The chain of custody must be maintained from the time of seizure to the presentation of evidence in court. This includes documenting the collection, transportation, and storage of the evidence, as well as the individuals who have handled it.

2) Preservation of evidence: The evidence must be preserved in its original state to ensure that it is not tampered with or altered in any way. This includes using appropriate storage methods and taking measures to prevent contamination or degradation of the evidence.

3) Handling of digital evidence: Digital evidence must be handled in a way that ensures its integrity and authenticity. This includes using appropriate tools and techniques for acquiring and analyzing the evidence, as well as creating a hash value of the evidence, which can be used to verify its integrity at a later time.

4) Documentation: Detailed and accurate documentation of the evidence-handling process is critical to ensure that the evidence is admissible in court. This includes documenting the tools and techniques used, as well as the results of the analysis.

5) Compliance with legal requirements: Forensic investigators must be aware of and comply with any legal requirements related to the handling of evidence. This includes ensuring that the evidence is collected and analyzed by the rules of evidence, as well as following any relevant laws or regulations regarding data privacy or jurisdiction.

Overall, proper evidence handling is essential for ensuring the integrity and admissibility of the evidence in a court of law. Forensic investigators must be well-trained and follow established protocols to ensure that the evidence is handled consistently and reliably.

D. Implementing forensic tools with Samsung Gear S3 in a cloud computing environment

It can have both benefits and consequences. Some of the potential consequences to consider include:

1) **Security risks:** Cloud computing environments can present security risks, such as unauthorized access to data or data breaches. This is especially true when it comes to sensitive data, such as evidence gathered during a forensic investigation. To mitigate these risks, it is important to ensure that the cloud environment is properly configured and that appropriate security measures are in place.

2) **Data privacy concerns:** Implementing forensic tools with Samsung Gear S3 in a cloud computing environment can raise concerns about data privacy. This is especially true if the cloud environment is operated by a third party, and if there is a possibility that the data may be stored or analyzed outside of the jurisdiction where it was collected.

3) **Jurisdiction issues:** It is important to consider jurisdiction issues when implementing forensic tools with Samsung Gear S3 in a cloud computing environment. This is especially true if the cloud environment is operated by a third party, and if there is a possibility that the data may be stored or analyzed outside of the jurisdiction where it was collected.

4) **Dependence on internet connectivity:** The use of cloud-based forensic tools can be dependent on the availability of internet connectivity. This can be a problem in some situations, such as when conducting a forensic analysis in a remote location or during a power outage.

5) **Legal admissibility:** Even though cloud-based forensic tools may be widely accepted and used, it is important to ensure that they are accepted and admissible in a court of law. This includes ensuring that the tools and techniques used are in compliance with legal requirements and that they are recognized as valid and reliable by the legal system.

6) **Cloud vendor lock-in:** Using a specific cloud vendor for forensic analysis can lead to vendor lock-in, where the organization is dependent on the vendor for the service, and it can be difficult to switch to another vendor.

Overall, implementing forensic tools with Samsung Gear S3 in a cloud computing environment can have benefits, such as increased storage capacity, remote access, and improved scalability, but it also presents new challenges, such as security risks, data privacy concerns, and jurisdiction issues. It's important to carefully evaluate these potential consequences and take appropriate measures to mitigate them.

E. Precautionary Measures needed to be taken during the acquisition

During the acquisition of digital evidence in a forensic investigation, it is important to take certain precautionary measures to ensure the integrity and authenticity of the evidence. Some of these measures include:

1) **Secure the scene:** Before beginning the acquisition process, it is important to secure the scene by ensuring that no unauthorized personnel are present and that the environment is controlled to prevent contamination of the evidence.

2) **Create an image of the evidence:** It is important to create an image of the evidence, such as a bit-by-bit copy of the entire storage device, to preserve the original evidence in its original state.

3) **Verify the integrity of the evidence:** The integrity of the evidence should be verified by checking the hash values of the original and the acquired image to ensure they match.

4) **Document the acquisition process:** The entire acquisition process should be well-documented, including the date and time of acquisition, the type of evidence, and the tools and techniques used.

5) **Use forensically sound tools:** Only use tools that are specifically designed for forensic acquisitions and that have been tested and proven to be forensically sound.

6) **Follow the chain of custody:** The chain of custody should be maintained at all times, and the evidence should be handled and stored in a secure and controlled environment.

7) **Use encryption:** Use encryption to protect the integrity of the evidence and to ensure that it is only accessible to authorized personnel.

8) **Labeling and packaging:** Label and package the evidence correctly to prevent any confusion or mishandling during the investigative process.

It's important to note that these are general guidelines and the specific acquisition procedures may vary depending on the type of evidence and the nature of the investigation.

VII. Conclusions & Furure Work

In conclusion, forensic analysis on cloud computing using Samsung Gear S3 can provide many benefits, such as increased storage capacity, remote access, and improved scalability. However, it also presents new challenges, such as security risks, data privacy concerns, and jurisdiction issues. To ensure a successful implementation, it is important to carefully evaluate these potential consequences and take appropriate measures to mitigate them. This includes ensuring that the cloud environment is properly configured that appropriate security measures are in place, and that the tools and techniques used are in compliance with legal requirements and are recognized as valid and reliable by the legal system. It's also important to consider the dependencies on internet connectivity, potential legal admissibility, and cloud vendor lock-in. Overall, by understanding and addressing these challenges, forensic analysts can effectively use cloud computing and Samsung Gear S3 to conduct forensic investigations and preserve the integrity of the evidence.

Several areas of future work can be considered when it comes to forensic analysis on cloud computing using IoT Samsung Gear S3. Some potential areas of focus include:

1) Developing new forensic tools: As technology continues to evolve, new forensic tools may be developed to take advantage of the capabilities of Samsung Gear S3 and other mobile devices. For example, new tools may be developed to analyze the data stored on the device or to extract data from the device's sensors, such as GPS or accelerometer data.

2) Improving security and data privacy: As more data is stored and analyzed in the cloud, it is important to continue to improve the security and data privacy of the cloud environment. This includes implementing measures to prevent unauthorized access to data, as well as ensuring that the data is stored and analyzed in compliance with legal and regulatory requirements.

3) Addressing jurisdiction issues: As more data is stored and analyzed in the cloud, it is important to continue to address jurisdiction issues. This includes ensuring that the data is stored and analyzed in compliance with legal and regulatory requirements and that the data is protected from unauthorized access or disclosure.

4) Enhancing cloud-based forensic analysis: Future work could aim at improving the scalability, reliability, and accessibility of cloud-based forensic analysis. This includes developing new techniques for analyzing large data sets, as well as improving the performance of existing techniques.

5) Developing standards: Developing standards for the proper use and handling of forensic data in cloud computing environments is important. These standards would help ensure the integrity and admissibility of the evidence in court.

Overall, there are many opportunities for future work when it comes to forensic analysis on cloud computing using IoT Samsung Gear S3. By continuing to develop new forensic tools and techniques, improving security and data privacy, addressing jurisdiction issues, and enhancing cloud-based forensic analysis, forensic analysts can continue to effectively use cloud computing and Samsung Gear S3 to conduct forensic investigations and preserve the integrity of the evidence.

References

[1] S. Achar, "Cloud computing forensics," *International Journal of Computer Engineering and Technology*, vol. 13, no. 3, 2022.

[2] H. F. Atlam, E. E.-D. Hemdan, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Internet of things forensics: A review," *Internet of Things*, vol. 11, p. 100220, 2020.

[3] F. A. Awan, "Forensic examination of social networking applications on smartphones," in *2015 conference on information assurance and cyber security (ciacs)*. IEEE, 2015, pp. 36–43.

[4] B. Cinar and J. P. Bharadiya, "Cloud computing forensics; challenges and future perspectives: A review," *Asian Journal of Research in Computer Science*, vol. 16, no. 1, pp. 1–14, 2023.

[5] A. M. Alenezi, "Digital and cloud forensic challenges," *arXiv preprint arXiv:2305.03059*, 2023.

[6] E. E.-D. Hemdan and D. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," *Multimedia Tools and Applications*, vol. 80, pp. 14 255–14 282, 2021.

[7] S. Rahman and M. Khan, "Review of live forensic analysis techniques," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 379–88, 2015.

[8] F. Iqbal, A. R. Javed, R. H. Jhaveri, A. Almadhor, and U. Farooq, "Transfer learning-based forensic analysis and classification of e-mail content," *ACM Transactions on Asian and Low-Resource Language Information Processing*, 2023.

[9] V. Prakash, A. Williams, L. Garg, C. Savaglio, and S. Bawa, "Cloud and edge computing-based computer forensics: Challenges and open problems," *Electronics*, vol. 10, no. 11, p. 1229, 2021.

[10] S. Raghavendra, P. Srividya, M. Mohseni, S. C. V. Bhaskar, S. Chaudhury, K. S. Sankaran, B. K. Singh *et al.*, "Critical retrospection of security implication in cloud computing and its forensic applications," *Security and Communication Networks*, vol. 2022, 2022.

[11] A. Regenscheid and K. Scarfone, "Recommendations of the national institute of standards and technology," *NIST special publication*, vol. 800, p. 155, 2011.

[12] Z. Chen, F. Han, J. Cao, X. Jiang, and S. Chen, "Cloud computing-based forensic analysis for collaborative network security management system," *Tsinghua science and technology*, vol. 18, no. 1, pp. 40–50, 2013.

[13] S. Pirzada, N. H. Ab Rahman, N. D. W. Cahyani, and M. F. Othman, "A survey of forensic analysis and information visualization approach for instant messaging applications," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 2, 2023.

[14] Z. Chen, F. Han, J. Cao, X. Jiang, and S. Chen, "Cloud computing-based forensic analysis for collaborative network security management system," *Tsinghua science and technology*, vol. 18, no. 1, pp. 40–50, 2013.

[15] F. Amato, A. Castiglione, G. Cozzolino, and F. Narducci, "A semantic-based methodology for digital forensics analysis," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 172–177, 2020.

[16] M. S. Mazhar, Y. Saleem, A. Almogren, J. Arshad, M. H. Jaffery, A. U. Rehman, M. Shafiq, and H. Hamam, "Forensic analysis on internet of things (iot) device using machine-to-machine (m2m) framework," *Electronics*, vol. 11, no. 7, p. 1126, 2022.

[17] A. Majeed and S. Saleem, "Forensic analysis of social media apps in windows 10," *NUST Journal of Engineering Sciences*, vol. 10, no. 1, pp. 37–45, 2017.

[18] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Systems with Applications*, vol. 190, p. 116198, 2022.

[19] F. Iqbal, A. R. Javed, R. H. Jhaveri, A. Almadhor, and U. Farooq, "Transfer learning-based forensic analysis and classification of e-mail content," *ACM Transactions on Asian and Low-Resource Language Information Processing*, 2023.

[20] D. Barrett, "Cloud based evidence acquisitions in digital forensic education." *Information Systems Education Journal*, vol. 18, no. 6, pp. 46–56, 2020.

[21] M. F. Hyder, S. H. Ahmed, M. Latif, K. Aslam, A. U. Rab, and M. T. Siddiqui, "Towards digital forensics investigation of wordpress applications running over kubernetes," *IETE Journal of Research*, pp. 1–16, 2023.

[22] S. Mishra, M. AlShehri *et al.*, "Forensics analysis of cloud-computing traffics," *International Journal of Computing and Digital Systems*, vol. 14, no. 1, pp. 1–xx, 2023.

[23] E. Khodayarseresht and S. Majumdar, "Digital forensics for emerging technologies: Present and future," in *Innovations in Digital Forensics*. World Scientific, 2023, pp. 1–11.

[24] Prachi and S. Kumar, "An effective ransomware detection approach in a cloud environment using volatile memory features," *Journal of Computer Virology and Hacking Techniques*, vol. 18, no. 4, pp. 407–424, 2022.

[25] S. Nasreen and A. H. Mir, "Enhancing cloud forensic investigation system in distributed cloud computing using dk-cp-ecc algorithm and ek-anfis," *Journal of Mobile Multimedia*, pp. 679–706, 2023.

Moayad Almutairi, Master student in Cyber Security & Digital Forensics ,IT Deptt. Majmaah University, Saudi Arabia. His research interests include cloud security, cybersecurity, the IoT, semantic web, cloud and edge computing, and smart city and mathematical modeling of physical and biological problems in general and mathematical analysis.

Shailendra Mishra, Shailendra Mishra (Senior Member, IEEE) received the Master of Engineering (M.E.) and Ph.D. degrees in computer science and engineering from the Motilal Nehru National Institute of Technology (MNNIT), India, in 2000 and 2007, respectively. He is currently working as Professor with the Department of Computer Engineering, College of Computer and Information Science, Majmaah University, Majmaah, Saudi Arabia. He has published and presented more than 90 research articles in international journals and international conferences. His current research interests include cloud and cyber security, SDN, the IoT security, communication systems, computer networks with performance evaluation, and design of multiple access protocol for mobile communication networks. He is a Senior Member of ACM, and a Life Member of the Institution of Engineers India (IEI), the Indian Society of Technical Education (ISTE), and ACEEE

Mohammed AlShehri, Mohammed Alshehri (Member, IEEE) received the B.S. degree from King Saud University, in 2001, the M.S. degree in computer and communication engineering from the Queensland University of Technology (QUT), Australia, in 2007, and the Ph.D. degree in information technology from Griffith University, Australia, in 2013. From 2002 to 2009, he was with the Ministry of Defense, Saudi Arabia, as an IT Manager, where he was a Consultant, from 2013 to 2015. He has been with Majmaah University, Saudi Arabia, since 2015, where he is currently Professor and Vice Rector ,Majmaah Universty. His research interests include span both computer science and information technology and applications to robotics in the field of education, cloud computing, artificial intelligence, and data science.