RESEARCH ARTICLE OPEN ACCESS

Survey on Locating and Retrieving Artifacts Remnant on Cloud Storage: Advancement and Future Direction

Hamza Audi Giade[1],Adamu Muhammad Tukur[2], Abdulaziz Saidu Yalwa[3]; Danlami Mohammed[4]

[1]Department of Computer science.Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: gidadohenz@gmail.com
[2]Department of Computer science. Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: babaadamu6644@gmail.com
[3]Department of Computer science. Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: abdulazizyalwaa@gmail.com
[4]Department of Computer science. Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: danlamimohd@gmail.com

--************************----------------------------

Abstract:

The majority of cloud computing research being done today focuses on minimizing challenges that forensic investigators can run into while trying to locate and retrieve artifacts from cloud devices. One of the challenges in locating and recovering artifacts from cloud settings is the variety of cloud service providers, each with its own set of regulations, specifications, and needs. In two key stages—the gathering of artifacts and the identification of evidence—this research suggests an inquiry strategy for finding and identifying data fragments. The suggested method locates the artifacts in cloud storage and gathers them in the artifacts collecting stage so that they may be examined further in the subsequent step. The gathered artifacts will be examined to find evidence pertinent to the cybercrime under investigation during the evidence identification step. These two phases will carry out a coordinated procedure to lessen the challenge of finding the artifacts and shorten the time required to find the pertinent evidence. The suggested method will be put into practice and evaluated by using the Windows 10 operating system to apply its algorithm to Sync cloud storage.

Keywords **—Digital forensics, Cloud company services, Sync cloud, cloud computing,**

--************************----------------------------

INTRODUCTION

As technology developed, cloud computing—also referred to as cloud storage—became more and more well-known because it offered a vast array of computer services to a large number of customers and organizations. Because cloud storage allows users to upload data to web servers, allowing instant access and the ability to share data with others at any time, cloud computing resources are frequently used by organizations to replace large housing computing systems, such as servers and data centers, in order to provide the highest level of access to data sources and also the availability of services to customers"A model for providing ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction," as stated by the National Institute of Standards and Technology (Mell and Grance, 2011). Cloud computing benefits small and medium-sized organizations by enabling them to obtain necessary computer services at a lower cost.

In addition, because of a pay-as-you-go approach that makes low-cost on-demand computing possible, businesses and IT organizations have more opportunities to test out premium services without having to pay for them up front since infrastructure resources are highly scalable.

However, because cloud technology allows data to be transferred or shared from one computer to another and opened on another without leaving much traceable evidence, it presents a difficulty for forensic investigators. Sync Cloud, iClouds, pClouds, Dropbox, Microsoft® SkyDrive, and Google Drive are just a few cloud storage services that are worth looking into more.

The National Institute of Standards and Technology (NIST) defines digital forensics as the application of science to the identification, collection, inspection, and analysis of data while guaranteeing data integrity and a stringent chain of custody. (Grance and Mell, 2011). The increasing legal obstacles that law enforcement will face when trying to gather or retrieve data from the cloud have so far been addressed by digital forensics. At that point, a lot of companies will ignore the legal implications of cloud computing. "In the event of a legal dispute, civil or criminal lawsuit, cyberattack, or data breach, how can my cloud provider provide me with digital forensics material?" is a concern that each organization using cloud-based services should think about. Network World is written by Messmer (2013). To collect digital evidence, the cloud provider must do each search on the requester's behalf. The next step is for the forensic investigators to ensure that the evidence they have acquired is authentic, reliable, comprehensive, compelling, and admissible. Due to the difficulty in determining what data was stored or processed by what software on what specific computing device, cloud computing systems may make it more difficult for a computer forensic analyst to gather and analyze digital evidence to the same standards as those currently expected for traditional server-based systems (Taylor et al,2011). The purpose of this study is to conduct a thorough and effective analysis of cloud clients alone, as opposed to cloud servers.to create a technique for locating data traces that might be useful in gathering digital artifacts from cloud client browsers.to create a procedure for dissecting the gathered artifacts and locating digital evidence pertinent to the cybercrime that was committed.Despite the advancement of cloud storage and the benefits it provides to all of us, we cannot ignore the fact that it is vulnerable to criminals who are able to use cloud computing services for criminal purposes, adding to the challenge of increasing volumes of digital evidence available on cloud storage in cases under investigation. With the rise in the number of crimes involving cloud storage, the use of cloud forensics as a means of obtaining the digital evidence needed by forensics investigators to investigate specific crimes involving cloud computing is becoming more complex. As a result, clients of public cloud services sought their cloud provider's help in conducting an investigation and retrieving digital evidence stored on clouds. The cloud provider must conduct each search on behalf of the requester in order to obtain the digital evidences. The forensic investigators must then guarantee that the evidence gathered is genuine, trustworthy, complete, convincing, and admissible. (Reilly, Wren, Berry).

To guarantee that all digital evidence collected is appropriate and acceptable for court hearings while also being understandable by jurisdiction personnel without IT backgrounds, it is critical to have a proactive methodology for conducting digital forensic investigations and examinations that is also flexible enough to work with future providers offering similar services (Quick and Choo). It's also critical for the forensics investigator to know where and what kind of data fragments cloud users leave behind on the devices they use to access their data.

This research used several objectives as shown below:

- To develop a method for identifying the location of data remnants that may help in collecting digital artifacts from cloud client browser.
- To develop a method for analyzing the collected artifacts and identifying digital evidence relevant to the committed cybercrime.

I. LITERATURE REVIEW

To find peer-reviewed literature on this study issue, a search was conducted. Because of this, a summary of the research results, methodology, limitations, and conclusions is given for each evaluated publication, and any conclusions that are similar or contradict each other are further addressed below.

Ming Sang Chang (2016) His primary objective was to locate data remnants on a Windows 10 computer through an examination of cloud activity on Amazon Cloud Drive and a search for evidence that could have been dropped by using different web browsers. In order to gather data that might have been overlooked as a result of these procedures, they used Amazon Cloud Drive, a cloud syncing service, as a case study. They also used a variety of Internet browsers and the EnCase application to analyze VMDK files that had been erased in order to improve the effectiveness of digital forensics and criminal investigations. Using a variety of web browsers, the researchers are investigating the cloud operations of Amazon Cloud Drive in an attempt to uncover any signals that could have been overlooked. The researcher's flaw was using the EnCase program, which is more expensive and takes a long time to process huge compound files than FTK, which is free and has more functionality. Only the username, cache files, and log activity are of interest to the researchers.

But in order to improve the effectiveness of digital forensics and criminal investigations, they don't concentrate on files that have been uploaded, downloaded, synced, erased, and so on.(Ming Sang Chang, 2016) Further study on Google Drive's cloud has been conducted by the same writers. The primary objective of the research was to locate data remnants on a Windows computer through an examination of Google Drive's cloud activities and an attempt to locate traces of these activities as well as other web browsers. As they noted, that will aid in improving the effectiveness of the digital forensics and crime investigation. They collected data that would have been overlooked as a result of these practices by utilizing the EnCase tool to analyze VMDK files and recover lost files. They did this by using Google Drive, a cloud syncing service, as a case study. In addition to examining Google Drive's cloud activity, the researchers are looking for any potential hints that may have been overlooked and different web browsers. They employed the EnCase program, which is quite costly and takes a long time when dealing with huge compound files. In contrast, FTK is speedier and offers more capabilities than EnCase. Researchers concentrate on data that is still in browsers; however, they ignore erased files, which are more significant and provide a difficulty for investigators in the modern day due to technological advancements. They also employed the EnCase program, which is quite costly and slow when dealing with huge compound files. In contrast, FTK is quicker and has superior capabilities than EnCase. Conversely, I learned that earlier studies (H. Kumar, R. Saharan, and S. K. Panda, 2020) had investigated whether Dropbox data could be uploaded, stored, and then retrieved. In order to create files in the Linux home and upload files from another operating system via Dropbox's website, which are synced and viewable in Linux as well, the researcher used Dropbox on Ubuntu 16.04 LTS to create a Dropbox account online, install it in this Linux machine, and sync it with the operating system. After that, they deleted their files and used Testdisk, a recovery tool, to recover the data. Using text files like.pdf and FileCreatedInLinux.txt that had been uploaded to Dropbox, they also used the terminal to create a FileCreatedInLinuxDropbox.txt file at the same place. The files then need to be deleted and reviewed. Files were erased with their attributes preserved by using the rm command on the terminal. You must use extreme caution while executing the rmcommand ..The Linux program PhotoRec was also utilized by the researchers in this study to recover data. Photorec is an open-source software that may be downloaded for free. It stores many file systems, including NTFS and ext3/ext4, in blocks. A tool called PhotoRec can retrieve data from files on a number of file systems that have been deleted or lost. Sectors of these blocks are kept at a certain place. For better efficiency, this data is continuously stored by all operating systems. There are several read and write operations in this approach.

In another test, they tried overwriting a memory region with a different file or set of data and found that even if the file was erased, the previous data could still be retrieved. This stage involves PhotoRec calculating the block size. The tool Photorec starts reading sectors and saves the first 10 files after finding that the file is corrupt. Block size is determined in part by these files. Block by block, data may then be retrieved from that point after that. To make sure they are recovered in the right format, these may be compared to the database. Their investigation led them to the conclusion that transferring large files to the designated location just takes a few seconds. On a hard drive, large data files might take several minutes to load. You may retrieve files ending in.mp3,.doc,.pdf,.mp4,.exe, and more extensions. Additionally, they found that a document they write on the Dropbox website instantaneously syncs with Linux. Libre Office may also be used to view and modify this document. Following testing, 97% of the files on Testdisk were successfully restored.The researcher found that several devices used to access or sync with the account are stored in the Dropbox app. You can also get the timestamps for every action it took with Dropbox, including installing, uploading, downloading, and deleting particular files and apps. In addition, the data retrieved by the tool's appropriate placement helped forensic investigators discover potential items in cloud storage applications. Conversely, a study conducted in 2016 by S. Easwaramoorthy, S. Thamburasa, G. Samy, S. Bhushan, and K. Aravind focused primarily on locating evidence data on a client computer and giving forensics practitioners a clear understanding of the kinds of evidence that are present in computers that have installed two different types of cloud providers (Amazon cloud drive and Microsoft One drive). This study aims to examine these forensic toolkits' efficacy and scientific validity in retrieving forensic evidence via Internet-based cloud computing settings. The data on a client computer provides a solid image of the kind of evidence that resides in computers, and the authors utilized this data to categorize the evidence for forensics specialists. Cloud service providers can access data timestamps, file hashes, client program log files, memory grabs, connection files, and other information found during this research. They collected forensic data on a Windows 7 machine using a browser and an application from the service provider, using two popular public cloud service providers (Microsoft One Drive and Amazon Cloud Drive). The researcher claims that several cloud service providers can also access file timestamps, link files, file hashes, memory grabs, client software log files, and other proof. Upon completion of the study, the researcher discovered that user account information could be located by investigators. This information will help investigators anticipate where user data may be found and take the necessary steps to promptly collect, assess, and preserve this evidence.

The authors find that the investigator may predict cloud storage account use data by carrying out a number of activities, including hash comparison, Registry analysis, RAM analysis, keyword searches, and network packet traffic analysis. The investigator would be able to obtain the username and password for the Mega account by analyzing network packet data, as well as the login credentials for OneDrive by gathering and examining a computer's RAM dump, according to their statement. In addition, study was done by (Thamburasa, et al., 2016) to learn more about the IDrive client software and the Mega cloud drive, as well as the types of evidence that these programs leave on a user's computer. For the purpose this research, the authors set up an IDrive account and a Mega cloud drive, uploaded and downloaded data, and then used forensic tools to completely delete the OS he was using. The remaining data was then retrieved from an image of the operating system.Li and Abdulrahman (2018) and Ahmed, C. X. found data evidence on client computers by researching pCloud and Dropbox on Windows 10 and Windows 7 OS. The objective was to give forensics practitioners a clear picture of the types of evidence that can be found on computers that have installed the two cloud providers (pCloud Drive and Dropbox Drive).

In this research, which discusses the many steps involved in gathering evidence on a user account using a browser and subsequently via cloud software program on a Windows 7 system (IDrive and Mega cloud drive), the authors analyze two cloud service providers.

Nonetheless, this study showed that items on a user's computer would provide investigators a broad idea of the kind of evidence remained in the user device. The primary evidence found during this study on a user's Windows PC from these two cloud providers includes RAM memory grabs, registry data, programme logs, file time and date values, and browser objects. In addition to this study, (S. Hraiz, 2017) also found that many researchers attempt to identify and solve cloud computing issues by putting out novel theories and methods, according to the authors.

The writers point out a few of these problems and discuss a number of potential solutions. Among the issues covered in their report were log files, volatile data, forensic image creation, and data integrity.

II. RESEARCH METHODOLOGY

The research focuses on the data's fate when a user uses Sync Cloud Drive to access, upload, and download it. We tested it with several browsers and the Sync Cloud Drive client application. Among the most popular browsers we use are Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer. We use different browsers in our research to investigate whether there are any differences in the ability to access data that still exists. Files, text within files, client software, users, and passwords are what we're searching for.

We also create scenarios where a user removes any traces of using Sync Cloud Drive by running the Eraser and CCleaner applications. We've looked closely at the various types of cloud service providers and the rules for looking into cybercrimes. We have spoken about some of them in earlier part of the research on how to retrieve data remains and where they could be discovered in Windows 10 operating system. As a result, detailed procedures that where applied to conduct this research was stated.

We employed the iterative waterfall model in this case.The iterative waterfall model essentially combines the regular waterfall model with the capability to repeatedly analyze each stage's operations until the optimal result is achieved. An iterative life cycle approach begins by specifying and implementing a subset of the program, as opposed to beginning with a full definition of requirements. After that, each component may be examined to find any other needs.

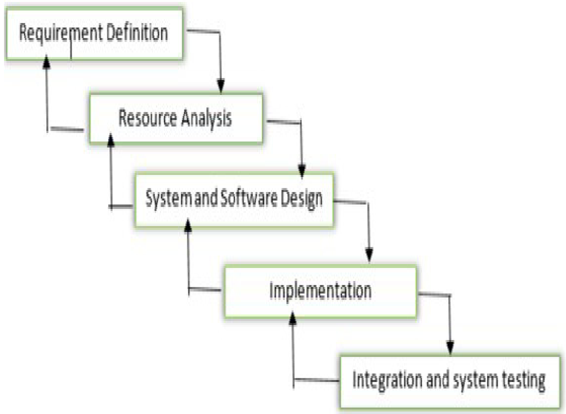


Figure 1: Iterative Waterfall Model

Iteratively, the process will start with a basic implementation of a portion of the software requirements and work its way up to a fully functional system version. To develop a fully working system, the design will be altered and new functionality will be added at each iteration stage. Resource analysis will come after the initial phases or processes of this model, which are requirement definitions, where needs for systems or research will be obtained. After that, I'll begin implementing the software and system design. Before proceeding to the integration and system testing phase, which is the last stage of the model, the implementation and unit testing procedures will be followed. The figure below shows the iterative waterfall process models.

Because the iterative waterfall model follows a step-by-step process and allows each stage to be completed within a predetermined time frame, it was selected. Additionally, we have a clear understanding of the needs for the entire system before we started the investigation. This is particularly important because the study project is big and has a number of important needs that need to be spelled out in detail. The approach and stages of each process should be regularly assessed as adjustments are made to accommodate all of the restrictions of the testing and other development procedures to make sure that they have all been addressed.

III. Resource Analysis

After gathering all the necessary materials, we examined each item of data to make sure it fits the research criteria and is relevant to building the application for this study. Any mistakes found in earlier stages where checked at this step to ensure that the mistakes have been fixed. Following that, all the data where completed in order to select the best approach to employ for this study.

As previously stated, in order to gather evidence in a consistent and forensically sound way, digital forensic practitioners and examiners should conform to commonly acknowledged standards, norms, and procedures.

Consequently, We have done this study in accordance with McKemmish's recommendations (McKemmish, 1999). We identified and described four phases in the forensics investigation process thanks to these principles, which require minimal handling of original evidences, accounting for all modifications, conforming to evidence norms, and not surpassing knowledge. These precise procedures include, but are not limited to, the identification, preservation, and analysis processes of digital evidence.

Finding prospective data is, as we all know, one of the most frequent issues that arise during the evidence analysis process. This is helpful because it tells forensic investigator examiners what information to look for when they suspect cloud storage—specifically, Sync cloud.

We will assemble a list of pertinent publications and previous research articles and critically examine them in order to obtain all of the necessary materials. In order to avoid the limitations We found in our own research, this study is essential for understanding the methodologies, goals, and study boundaries that were employed. The research also includes determining if the data that remains will be successfully detected. The data is concealed using anti-forensics techniques to conceal indications of cloud storage usage.

The cloud storage that is being used, the username and password that were entered, and any files related to the use of the cloud account that might be crucial to the investigative techniques should all be included in the resources that are found. This will help me as I do this study. Furthermore, We collected information on the many kinds of cloud service applications to elucidate their diverse benefits and drawbacks overall.

A. *Analyzing software and hardware requirement*

Prior to proceeding to the design stage, the study also entails research and analysis of hardware, software, and a few key programming languages. Prior to developing the entire system, the platform analysis process is essential since every platform has a unique system architecture and set of kernel functions. The specific program that I would need to carry out this research is listed in the table below.

TABLE I

SOFTWARE REQUIREMENT

Software Required	**Description**
VMWare Player	For testing purposes, a virtualized desktop is used to run an operating system.
Multiple browser including Microsoft Edge(ME), Google Chrome(GC) and Mozilla Firefox(FF)	To create and access sync cloud application account in a range of ways including different browsers.
CCleaner	To erase specific files
Eraser	To erase specific files
Sync cloud application	To gain access to the information saved in the cloud application.
FTK Imager	E01 files for each VM is created using this tool.
Encase & FTK	Use to analyzing the images from VM
Wireshark's	To capture the PCAP files
Process Monitor	Use to keep track of changes to files and the registry.
Window 10 Pro 64bit	Platform for research project development

Microsoft Word	Drafts of proposal and write document
Microsoft Project	planning Gantt chart
Microsoft Visio	To create all of the required diagrams

TABLE II

HARDWARE REQUIREMENT

Specifications	Description
Laptops (ASUS K43SD, Intel Core i5 2450M 2.5GHz, 6GB DDR3 SDRAM, 2.5" SATA 500GB 5400rpm)	Used for the whole research project that included documentation and result comparison. .
External Hard Disk of Toshiba 500GB	To back-up project files
16 GB Kingston thumb drive	To transfer files

B. *System Configuration*

Using Sync Cloud as a case study, we created 21 virtual machines to gather the data and information required to address the research issue. In order to compare the outcomes, we set up a few alternative scenarios, such as accessing Sync using Google Chrome (GC), Mozilla Firefox (FF), and Microsoft Edge (ME). Table 3 illustrates how many Virtual Machines (VMs) were built for every browser to replicate different use patterns.

In order to limit the amount of storage space required for the quantity of virtual devices and forensic photos I created throughout the testing, the basic systems were designed with 20GB of RAM and hard drive space. Reducing the amount of time needed to analyze the test-generated data is another goal. Third, the belief was that there was a greater chance that pertinent data would be discovered on the larger system if it could be located on smaller systems. Essentially, SysInternals Process Monitor will be used to monitor system changes in the virtual machine.

However, studies have revealed that forensic photographs and memory grabs utilizing SysInternals Process Monitor are contaminated with a significant amount of data on both memory captures and hard disk pictures. Thus, SysInternals Process Monitor was not used in this investigation. It could detect modifications to file systems and registry files by comparing base image files with subsequent image files to determine the changes made.

TABLE III

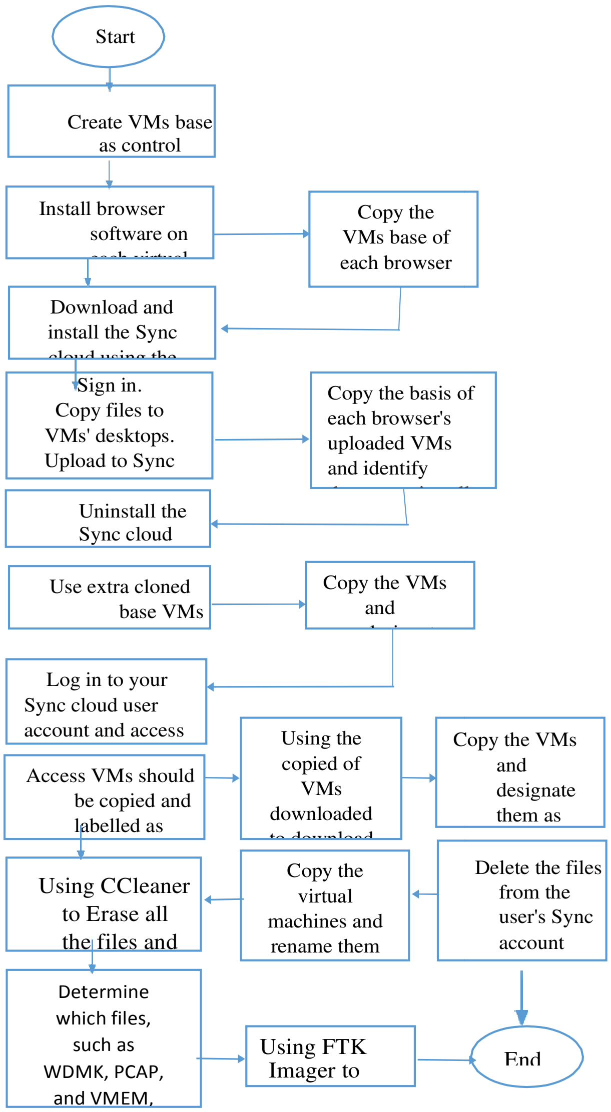
TYPES OF VMS NEEDED

Virtual Machines	Details
Base-VM which includes ME, MF and GC	2 GB RAM, 20 GB Hard Disk Drive, Windows 10 Home Basic SP1. Microsoft Edge(ME), Mozilla Firefox (FF), and Google Chrome are the browsers that are installed for each test (GC).
Upload-VM ME, GC, and FF	Download and instal the Sync cloud Windows Client programme. The test account has been accessed. Data from Enron was uploaded to a user's Sync cloud account.
Uninstall-VM ME, FF and GC	Uninstall the Sync cloud client programme utilising the Upload-VM via the Windows Start Menu option.
Access-VM ME, GC and FF	Browser used to sign in to the user test account on the Sync cloud website at www.sync.com. Each file in the Sync cloud account storage was accessed but not downloaded on purpose.
Download-VM ME, GC and FF	Browser used to sign in to the user test account on the Sync cloud website at www.sync.com. Each file was downloaded and opened on the VM Hard Drive Desktop.
Eraser-VM ME, GC and FF	The Sync cloud and Enron data were deleted using Eraser software on each copy of the Download-VMs.
CCleaner-VM ME, GC and FF	Each copy of the Eraser-VMs had CCleaner downloaded, installed, and run with default parameters.

C. *System Design*

All of the examined data will be converted into a flowchart format at this stage. We will be able to utilize all of the requirements that have been analyzed and the data that has been acquired throughout the requirement definition and analysis phase to our research when we apply it to the system design phase. I may create the general process flow that will be used in the implementation phase later on when I construct the system. In order to obtain the required findings for us within the time range I have specified, this will also be used to guide us through every experiment I have planned.

In order to save time, it also provides a concept of how I would conduct our study experiment going forward. In addition, the information I acquired enables us to standardize the requirements needed or carrying discover our method for conducting study experiments. With this data, I can create a flowchart that will show how I will test the components later and how the experiment should be carried out throughout our trial. Figure 2 below depicts the flowchart of the entire procedure to be followed throughout this experiment.


Start
Create VMs base as control
Install browser software on each virtual
Copy the VMs base of each browser
Download and install the Sync cloud using the
Sign in. Copy files to VMs' desktops. Upload to Sync
Copy the basis of each browser's uploaded VMs and identify
Uninstall the Sync cloud
Use extra cloned base VMs
Copy the VMs and
Log in to your Sync cloud user account and access
Access VMs should be copied and labelled as
Using the copied of VMs downloaded to download
Copy the VMs and designate them as
Using CCleaner to Erase all the files and
Copy the virtual machines and rename them
Delete the files from the user's Sync account
Determine which files, such as WDMK, PCAP, and VMEM,
Using FTK Imager to
End

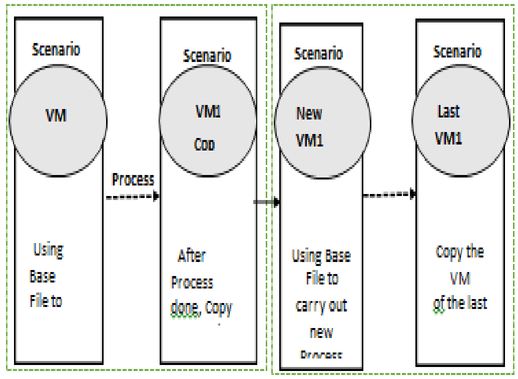


Figure 3: VM use during scenario execution.

Figure 2: Flow chart of the experiment.

Furthermore, the flowchart was employed to guide the implementation of prearranged experiment scenarios with the aim of achieving the desired result within a designated timeframe. This method also provided an overview of the experiment's execution, so as to minimize time wastage. To ensure that every scenario was created in a new virtual machine environment and that precise data was gathered, each method used brand-new virtual machines (VMs) that were cloned, deleted, and reinstalled after testing. In the recently created virtual machines, the subsequent scenarios were examined. The scenario's utilization of virtual machines (VMs) is shown in Figure 3.

D. *Implementation Phase*

As previously said, every detail specification that was obtained during the system design step was required for the implementation stage. The phases that are finished will then be applied in the real experiment. To reach a conclusion, the experiment will be carried out using the 21 virtual machines (VMs) that we previously mentioned. In order to finish all of the tests as quickly as possible without wasting any resources, three to four virtual machines will be assigned to each of the six testing computers. To ensure that everything could run properly, a quick study of the exact requirements and design specifications was necessary before the real-time experiment was conducted.

All necessary hardware and software components will be ready before the integration and system testing phase begins to prevent any unnecessary issues that might end up stopping the testing process later.

E. Integration and System Testing

The final stage of the study process will be integration and system testing. This stage involves software testing, when separate software components are combined and tested collectively. It takes place in between validation and unit testing. Therefore, we will use the previously intended method to separately test each of our functionalities in this study. The purpose of this experiment and testing is to address the issue statement that was identified during the requirement formulation stage.

To ensure the correctness of the findings and assertions made in the earlier research, the main goal of this testing is to illustrate our study utilizing a real-time process. Furthermore, the testing stage will be able to pinpoint every experiment's weak point and constraint, enabling us to make improvements to get the intended result.

In system or software development, alpha testing takes place during the integration and testing phase. Prior to beta testing, commercial off-the-shelf software (COTS) is often put through alpha testing as a form of internal acceptance testing. All of these will facilitate the research process. Using this iterative waterfall method, any minor function modifications can still be completed and reviewed before or after alpha testing.

IV. COMPARATIVE ANALYSIS

One of the objectives of this study was to effectively test and develop a technique for locating locations and data fragments left on a user's computer before utilizing a cloud storage application for fresh cloud storage. The research by (AHMED AND XUE LI, 2018a) utilizing pCloud as their case study covers the analysis of VM Cache files and related files, which was proven in acquiring information on the history of files ran on user's machine before.

Nevertheless, our research has revealed a wealth of useful information, such as usernames, passwords, cached files, and deleted files. Additionally, we are aware of the exact location of this useful information, which may help cloud security investigators look into cloud synchronization that may be connected to criminal activity.

Moreover, the directory listing of Sync Cloud showed that synced files existed that matched the files found in sync Cloud accounts, helping forensic investigators to gather evidence offline. The "cfg.db" files produced by Sync Cloud include more information than the "filecache.dbx," "host.db," or "data.db" files produced by Dropbox and pCloud, according to the current study's investigation of a client application. The "cfg.db" file from Sync Cloud included details on the local path of Sync Cloud sync, the number of ports used to access it, and web surfing statistics. On the other hand, "filecache.db," "host.db," and "data.db" included simply the pCloud user account login and a history of filenames synced with Dropbox.

V. CONCLUSION

As technology advances, cloud computing and cloud storage services have become more widely accepted and well-liked since they are practical for people everywhere. Cloud computing, however, is making it more challenging for forensic investigators to handle data related to criminality. This is because data may be read and uploaded from several devices simultaneously without creating a trace. Consequently, figuring out what kind of cloud service providers Posed a major challenge to researchers.

The objectives of this research was restricted to the Sync Cloud case study. Future studies using the same methods are required to investigate the other recently launched cloud storage providers that have just entered the market. This is to see if this technique is appropriate for use with other cloud service providers.

In addition, plans exist for additional research to expand the scope of the study to encompass more studies including tablets and mobile devices that are synced with cloud service accounts. In addition, there will be opportunities for future research to test and experiment with the newest operating systems, such as Windows 11 crucial user data needed to support the investigation, as well as the tools used by thieves. This will make it easier for forensic investigators to find important data and to extract and preserve it in a way that adheres to forensic best practices.

REFERENCES

[1] A. A. Ahmed and C. X. Li, "Locating and Collecting Cybercrime Evidences on Cloud Storage: Review," International Conference on Information Science and Security (ICISS), 2016, pp. 1-5, doi: 10.1109/ICISSEC.2016.7885861, 2016

[2] Abdulrahman K., Ahmed A.A., Mohammed M.N. "Investigation Model for Locating Data Remnants on Cloud Storage". 2019

[3] Vasant P., Zelinka I., Weber GW. (eds) "Intelligent Computing & Optimization. ICO Advances in Intelligent Systems and Computing", vol 866. Springer, 2018.

[4] Ahmed, A.A., Li, C.X.: "Analyzing data remnant remains on user devices to determine probative artifacts in cloud environment". J. Forensic Sci. 63(1), 112–121, 2018

[5] Ahmed, A.A.: "Investigation approach for network attack intention recognition". Int. J. Digit. Crime Forensics (IJDCF), 2017

[6] AmeerPichan, MihaiLazarescu, SieTeng Soh. "Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation" 2015;13:38-57. 2018.

[7] Biggs, S &Vidalis, S. "Cloud Computing: The Impact on Digital Forensic Investigations". Proceedings of IEEE International Conference for Internet Technology and Secured Transactions. 2009;1–6. 2018.

[8] Chang, Ming Sang. "Forensic Analysis of Google Drive on Windows." IJISET- International Journal of Innovative Science, Engineering & Technology 3.8 2016

[9] Chang, Ming Sang. "Forensic investigation of Amazon Cloud Drive on Windows 10". IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016

[10] Darren Quick, Kim-Kwang Raymond Choo, "Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?", Science direct, Digital Investigation, vol. 10, Issue 3, pp. 266-277, October 2013.

[11] Denis Reilly, Chris Wren, Tom Berry, School of Computing and Mathematical Sciences, "Cloud Computing: Pros and Cons for Computer Forensic Investigations", https://www.researchgate.net/publication/228458052_Cloud_Computing_Pros_and_Cons_for_Computer_Forensic_Investigations

[12] Guo, H, Shang, T & Jin, B. "Forensic Investigations in Cloud Environments". IEEE International Conference on Computer Science and Information Processing. 2012;248- 251.

[13] H. kumar, R. Saharan and S. K. Panda, "Identification of Potential Forensic Artifacts in Cloud Storage Application," International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020, pp. 1-5, doi: 10.1109/ICCSEA49143.2020.9132869, 2020.

[14] Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications,42(21):7905–7916, 2015

[15] Messmer, E. (2013, March 6). "Cloud forensics: In a lawsuit, can your cloud provider get key evidence you need? Network World. Retrieved from http://www.networkworld.com/news/2013/030613-cloud-forensics-267447 2013

[16] Naomi Euide, CIODIVE, Cloud market potential unbound as 'cloud-first' becomes ubiquitous, 2021

[17] NIJ. "Electronic crime scene investigation: a guide for first responders". 2nd edition. Retrieved from National Institute of Justice (NIJ): http://www.nij.gov/pubs- sum/219941 . 2001.

[18] NIJ. NIJ. Retrieved from Electronic crime scene investigation: a guide for first responders. 2nd edition.: http://www.nij.gov/pubsum/219941 (2008);2008

[19] Peter Mell, Timothy Grance, NLST, The NIST Definition of Cloud Computing https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[20] Purnaye, Prasad &Kulkarni, Vrushali. "A Comprehensive Study of Cloud Forensics. Archives of Computational Methods in Engineering". 10.1007/s11831-021- 09575-w. 2021

[21] S. Easwaramoorthy, S. Thamburasa, G. Samy, S. B. Bhushan and K. Aravind, "Digital forensic evidence collection of cloud storage data for investigation," International Conference on Recent Trends in Information Technology (ICRTIT), 2016, pp. 1-6, doi: 10.1109/ICRTIT.2016.7569516, 2016.

[22] S. Hraiz, "Challenges of digital forensic investigation in cloud computing," 8th International Conference on Information Technology (ICIT), 2017, pp. 568-571, doi: 10.1109/ICITECH.2017.8080060, 2017

[23] S. Thamburasa, S. Easwaramoorthy, K. Aravind, S. B. Bhushan and U. Moorthy, "Digital forensic analysis of cloud storage data in IDrive and Mega cloud drive," International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-6, doi: 10.1109/INVENTIVE.2016.7830159, 2016

[24] Samy, G. N., Maarop, N., Abdullah, M. S., Perumal, S., Albakri, S. H., Shanmugam, B., & Jeremiah, P. "Digital forensic investigation challenges based on cloud computing characteristics". International Journal of Engineering and Technology(UAE), 7(4.15), 7-11. https://doi.org/10.14419/ijet.v7i4.15.21361 2018.

[25] Simou, S., Kalloniatis, C., Gritzalis, S., and Mouratidis, H. "A survey on cloud forensics challenges and solutions". Security Comm. Networks, 9: 6285– 6314. doi: 10.1002/sec.1688. 2016

[26] STAMFORD, Conn, Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021, gartner, November 17, 2020.

[27] Taylor, Mark & Haggerty, John &Gresty, David & Lamb, David. "Forensic investigation of cloud computing systems".Network Security. 2011. 4-10. 10.1016/S1353-4858(11)70024-1. 2011