Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 1810 – 1821

A Comparative Analysis of Various Forensic Tools used in Secure Digital Transmission

Aakriti Saini[1], Mr. Dheeraj Kapoor[2], Dr. Meenu Manchanda[3], Dr. Pankaj Gupta[4],Dr. Deepak Goyal[5]

Abstract

A forensic methodology is presented for examination huge size of log records to extricate information which can help advanced specialists and inspectors during the examination of cloud based crimes that happened through a specific time. In this methodology, we utilized Apache Hadoop and Apache Spark for investigation web log information. Apache Hadoop for examination of log information is utilized while an Apache Spark is utilized to give bunch and constant investigation of 200 web worker log information. In each approach, three unique projects are carried out and tried on three distinctive log documents in size. Each program extricates the diverse kind of data that can help advanced examiners in remaking timetable related crimes that are happened. The outcomes show that Apache Hadoop and Apache Spark can be utilized as quick stages for preparing different enormous size of log documents and concentrate valuable data that can uphold computerized examiners in investigation monstrous measure of cloud log information in a given edge time just as remade course of events identified with occurrences. Besides, the outcomes can arrangement to remake and produce a timetable identified with verifiable past grouping occasions happened during a crime just as distinguish the malignant client's IP address, date and time, with the quantity of access.

Keywords: Digital Evidence, Computer Forensics, Digital Forensics

1. Introduction

Computerized proof is the source information that assistance and help advanced specialists for cybercrimes examination and assessment to carry the crooks to judgment. The advanced proof might be in different structures like content, sound, picture, and video. In the courtroom, the proof used to demonstrate and build up that cybercrime or occurrence has been carried out or can convey a connection between a crime and its casualty [1]. Figure 1 shows various sorts of advanced proof.

[1] M.Tech Scholar, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, saini.aakriti0480@gmail.com

[2] Assistant Professor, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak,kapoordhiraj79@gmail.com

[3] Professor,Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak,meenumanchanda73@gmail.com

[4] Professor, Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak,pankajgupta.vce@gmail.com

[5] Professor, Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, deepakgoyal.vce@gmail.com

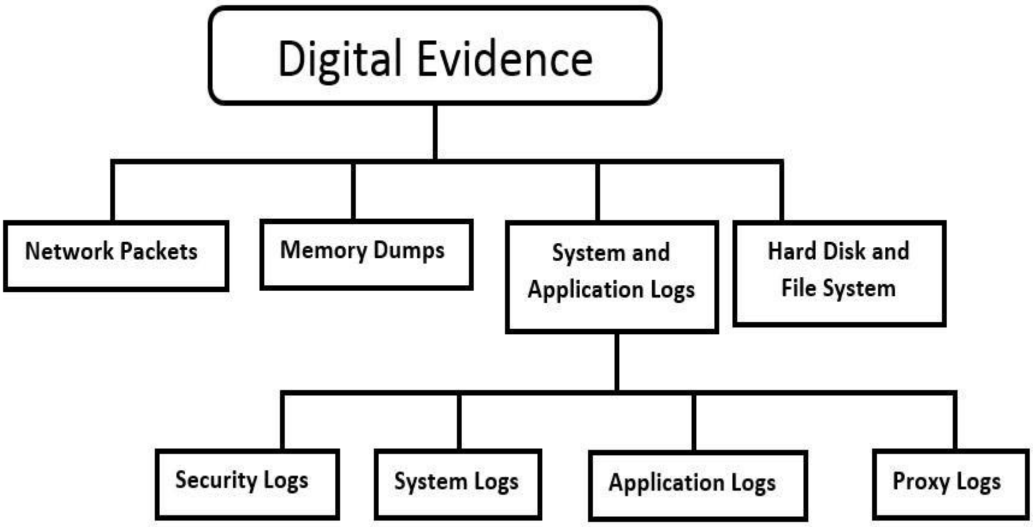


Fig.1 Digital Evidence Types.

Cyber Crimes: In the new time, cybercrimes become more basic as dangers for breaking framework security because of creative thoughts that crooks have with respect to groundbreaking thoughts and approaches to carries out these crimes. The hoodlum's abuse weaknesses of new advances to carry out their crimes such that make it is hard to find and follow them back [3]. The powerful idea of distributed computing adds to the issues met by specialists while separating and getting ready computerized proof for a courtroom.

Cyber Crime Classification in Computer Forensic: Cybercrime is classified as the following [9]:

- The PC as an objective: The criminal tries to keep the authentic clients or proprietors from getting the framework admittance to their information or PCs like Denial of Service (DOS) assaults.
- The PC as an apparatus of the crime: The PC is utilized to acquire some other criminal target. For instance, a criminal may utilize a PC to take individual data.
- The PC as accidental to a crime: The PC isn't the essential instrument of the crime; it just works with it.
- Crimes related with the commonness of PCs: This incorporates crimes against the PC business, like programming theft.

Cyber Crime Classification in Cloud Forensic: In the cloud computing environment, cyber-crimes divided into two main types:

- Crimes using the cloud infrastructure resources capacities to be performed the malicious attacks.
- Crimes against the cloud infrastructure**.**

2. Cloud Forensıcs

The term of cloud forensics was presented by Ruan et al. [2012] to distinguish the quickly arising need for advanced forensics in the cloud. She characterized cloud forensic as a cross-control of distributed computing and computerized forensics. Likewise, referenced that in "Cloud forensics is a subset of organization forensics Organization forensics manages forensic examinations of organizations. Distributed computing depends on expansive organization access. In this manner, cloud forensics follows the principle periods of organization forensics with strategies custom fitted to distribute computing conditions".

Ruan's functioning meaning of cloud forensics is: "Cloud forensics is the utilization of computerized forensic science in distributed computing conditions. Actually, it comprises of a mixture forensic methodology (e.g., distant, virtual, network, live, huge scope, slight customer, thick-customer) towards the age of computerized proof. Hierarchically it includes communications among cloud entertainers (i.e., cloud supplier, cloud purchaser, cloud representative, cloud transporter, cloud reviewer) to work with both inside and outer examinations [5]. Legitimately it frequently suggests multi-jurisdictional and multi-occupant circumstances"

Cloud Forensics Challenges

- Entertainer/Stakeholder: This variable [a noun] distinguishes the stakeholder(s) who are influenced by the test that has been recognized. Instances of partners incorporate cloud customers, examiners, specialists on call, and so on
- Activity/Operation: This variable [a verb] recognizes the movement that the partner might want to perform. Instances of activities incorporate decoding, imaging, getting entrance, and so forth
- Object of This Action: This variable distinguishes the particular thing whereupon the activity is to be performed. Instances of items incorporate information, review logs, timestamps, proof, and so forth
- Reason: This variable recognizes the essential difficulties that the partner faces to play out the predefined activity on the item.

The standardized portrayal of certain difficulties is:

For forensic inspectors, recognizing and crediting information that is erased in the cloud to a particular client is a test in light of the fact that the sheer volume of information and clients continually working in a cloud climate restricts various reinforcements that the cloud Provider will hold. For specialists, connection of action is a test on the grounds that there is no interoperability between cloud Providers [8]. For all specialists and courts, reproduction of virtual pictures or capacity is testing on the grounds that these recreation calculations should be approved or created. For agents/law authorization/examiners, the assortment and conservation of forensic proof is testing in light of the fact that there is an absence of interoperability among suppliers and there is absence of control from the client's viewpoint into the restrictive engineering and additionally the innovation utilized. For law implementation, guaranteeing legitimate chain of guardianship and security of information, metadata, and perhaps equipment is a test since it could be hard to decide possession, authority, or precise area.

Engineering: In cloud forensics, the design difficulties remember managing fluctuation for cloud models between suppliers; inhabitant information compartmentalization and segregation during asset provisioning; expansion of frameworks, areas and endpoints that can store information; precise and secure provenance for keeping up and protecting chain of authority; foundation to help capture of cloud assets without upsetting different occupants; and so forth

Information assortment: Challenges of information assortment remember finding forensic antiques for enormous, dispersed and dynamic frameworks; finding and gathering unpredictable information; information assortment from virtual machines; information respectability in a multi-occupant climate where information is divided between numerous PCs in various areas and available by different gatherings; powerlessness to picture every one of the forensic relics in the cloud; getting to the information of one inhabitant without breaking the privacy of different inhabitants; recuperation of erased information in a common and appropriated virtual climate [10]

Investigation: Analysis challenges in cloud forensics incorporate connection of forensic curios across and inside cloud suppliers; remaking of occasions from virtual pictures or capacity; trustworthiness of metadata; timetable examination of log information including synchronization of timestamps; and so forth

Hostile to forensics: Anti-forensics is a bunch of methods utilized explicitly to forestall or deceive forensic investigation. Difficulties in cloud forensics incorporate the utilization of obscurity, malware, information covering up, or different procedures to bargain the respectability of proof; malware may evade virtual machine confinement strategies; and so forth

Job the executives: Role the board difficulties in cloud forensics incorporate interestingly distinguishing the proprietor of a record; decoupling between cloud client qualifications and actual clients; simplicity of obscurity and making imaginary personalities internet; deciding definite responsibility for; validation and access control; and so on

Legitimate: Legal difficulties in cloud forensics incorporate distinguishing and resolving issues of locales for lawful admittance to information; absence of successful channels for worldwide correspondence and participation during an examination; information obtaining that depends on the collaboration of cloud suppliers, just as their

Skill and Reliability; missing terms in agreements and administration level arrangements; giving summons without information on the actual area of information; seizure and seizure of cloud assets may intrude on business coherence of different inhabitants; and so on

Principles: Standards challenges in cloud forensics incorporate absence of even least/essential SOPs, practices, and devices; absence of interoperability among cloud suppliers; absence of test and approval techniques [12]

Preparing: Training difficulties in cloud forensics incorporate abuse of computerized forensic preparing materials that are not relevant to cloud forensics; absence of cloud forensic preparing and skill for the two agents and teachers; restricted information by record-keeping staff in cloud suppliers about proof; and so on

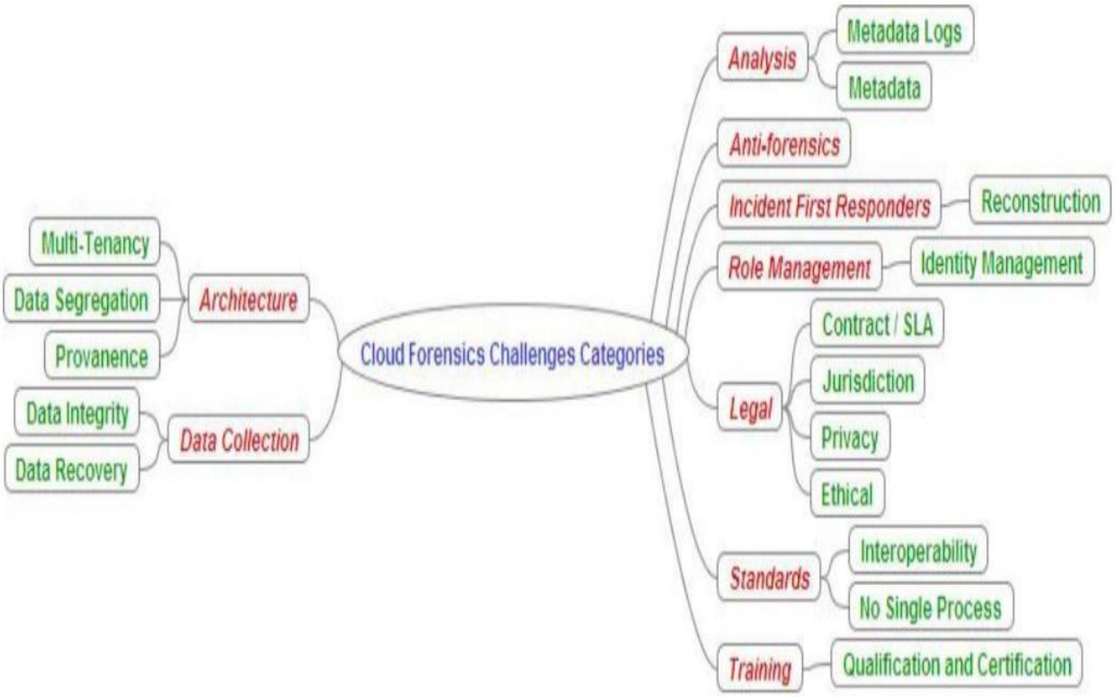


Fig.2 Cloud Forensics Challenges Categories

3. Cloud Forensics Opportunities

The digital forensic investigation has various opportunities to be applied in cloud computing environment as follow:

Practical: Implement forensic assistance in distributed computing climate that permit using the immense limits of distributed computing without move the advanced proof from the cloud to the opposite side to play out the examination cycle which needs high data transfer capacity.

Information bounty: Replication of information in cloud climate presents the fundamental chance for cloud forensic for recuperate the lost and erased information from the cloud to confirmation the crime.

Versatility and adaptability: Cloud forensic administrations can use the offices of adaptability and adaptability asset use, for instance, giving limitless stockpiling, process and organization assets with the compensation per-use strategy.

Approaches and Guidelines: Develop new principles and strategies for cloud forensic science because of quick difference in the innovation of distributed computing and cybercrimes against it.

Forensics as a Service (FaaS): Cloud registering gives one incredible alternative to computerized agents and inspectors called Forensic as a Service (FaaS). The forensic examiner can convey the FaaS through using the huge cloud capacities. This assistance makes advanced forensics as an "on-request" administration for permitting monstrous capacity and processor power as important to direct a computerized examination of crimes. Forensic workers will dwell on the cloud side, disconnected, until require emerges for them. Reports could be upheld into the cloud for the computerized specialists to use without upsetting typical business [8]. Without a doubt the cloud assets could be utilized for arranging, looking, and hashing the proof information. There are numerous advantages of the Forensic as a Service as follows:

- Decrease proof securing time: If a worker in the cloud is undermined, it tends to be cloned and made promptly accessible to a cloud forensics worker.
- Diminish administration personal time: Due to the equipment deliberation in the cloud, particular equipment won't need to be gotten to proceed with the procurement of the proof in certain circumstances.
- Lessen proof exchange time: The mists conveyed record framework considers making quick piece for-bit duplicates.
- Decrease forensic picture confirmation time: Some cloud conditions utilize a cryptographic checksum or hash that can definitely diminish the time needed to hash records disconnected
- Decline time to get to secured records: The pooling of CPU power accessible in the cloud can make unscrambling a lot quicker.
- Essentially limitless log stockpiling: Cloud stockpiling arrangements will make the requirement for assessing how much plate space is required for logging superfluous, taking into account a lot of log information to be kept and utilized during an examination.
- Improve log ordering and searches: Along with limitless capacity, logs can be filed and looked through successfully progressively with cloud assets.

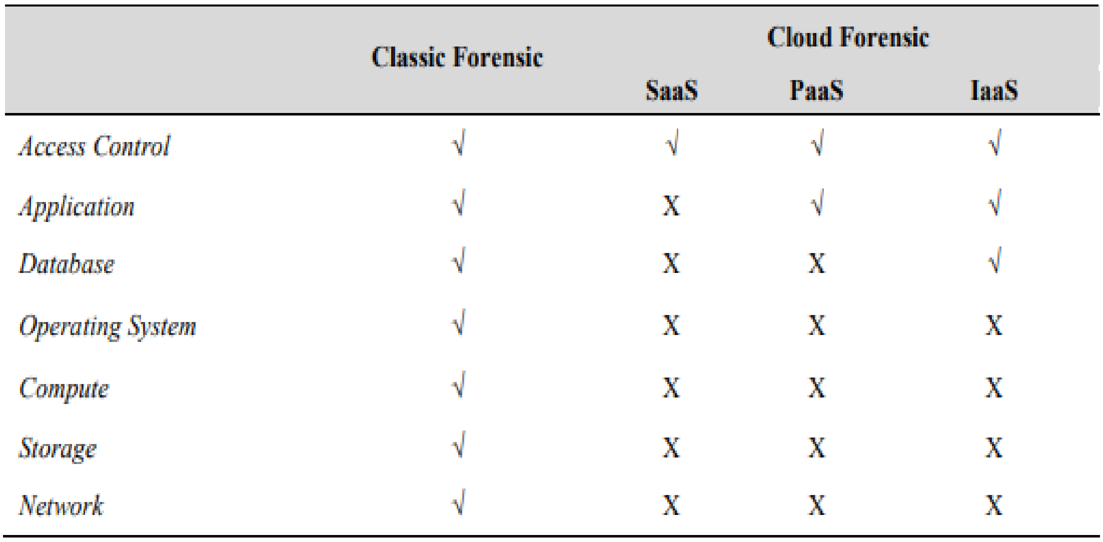
4. Comparıson between Tradıtıonal Computer Forensıc and Cloud Forensıc

Current Research Problems in Cloud Forensics: In this division, a study of open problems and impediments in cloud forensics will discuss as follows: Collection and Acquisition of Forensic Data, Log Information, Service Level Agreement (SLA), Virtual Machine Introspection (VMI), Data Provenance in Cloud, Trusted Platform Module (TPM), Isolating a Cloud Instance and Forensic Analysis for Cloud Storage Services [6].In Table , a comparison study between Classic Forensic and cloud forensic is tabulated to explain the differences between both above two types of forensics.

Enlightening Metadata: Descriptive metadata contains indispensable data about an advanced item like creator, title, association, and watchwords. The enlightening metadata is utilized for delivering and dealing with a gathering of advanced items, like looking through distributed sections.

Underlying Metadata: This metadata portrays how compound advanced items are assembled and the connection between the parts. The primary metadata is utilized for the computerized object show and route through its few sections.

Table 1 Comparison between Computer Forensic and Cloud Forensic



	Classic Forensic	Cloud Forensic		
		SaaS	PaaS	IaaS
Access Control	√	√	√	√
Application	√	X	√	√
Database	√	X	X	√
Operating System	√	X	X	X
Compute	√	X	X	X
Storage	√	X	X	X
Network	√	X	X	X

5. Methodology

The proposed approach fills in as a direct preventive registration in the honesty of client information in distributed storage, for example, Box distributed storage, then, at that point, if there is any progressions or changes and altering the client information that put away in distributed storage supplier, then, at that point the advanced examiners and specialists will begin playing out the computerized examination measure. This methodology will assist with protecting client's information with saving time and cost of the entire examination measure. The proposed framework can give notice while a few sorts of progress or modifying of information happened, on account of the warning; it is not difficult to distinguish the crime against cloud client's information.

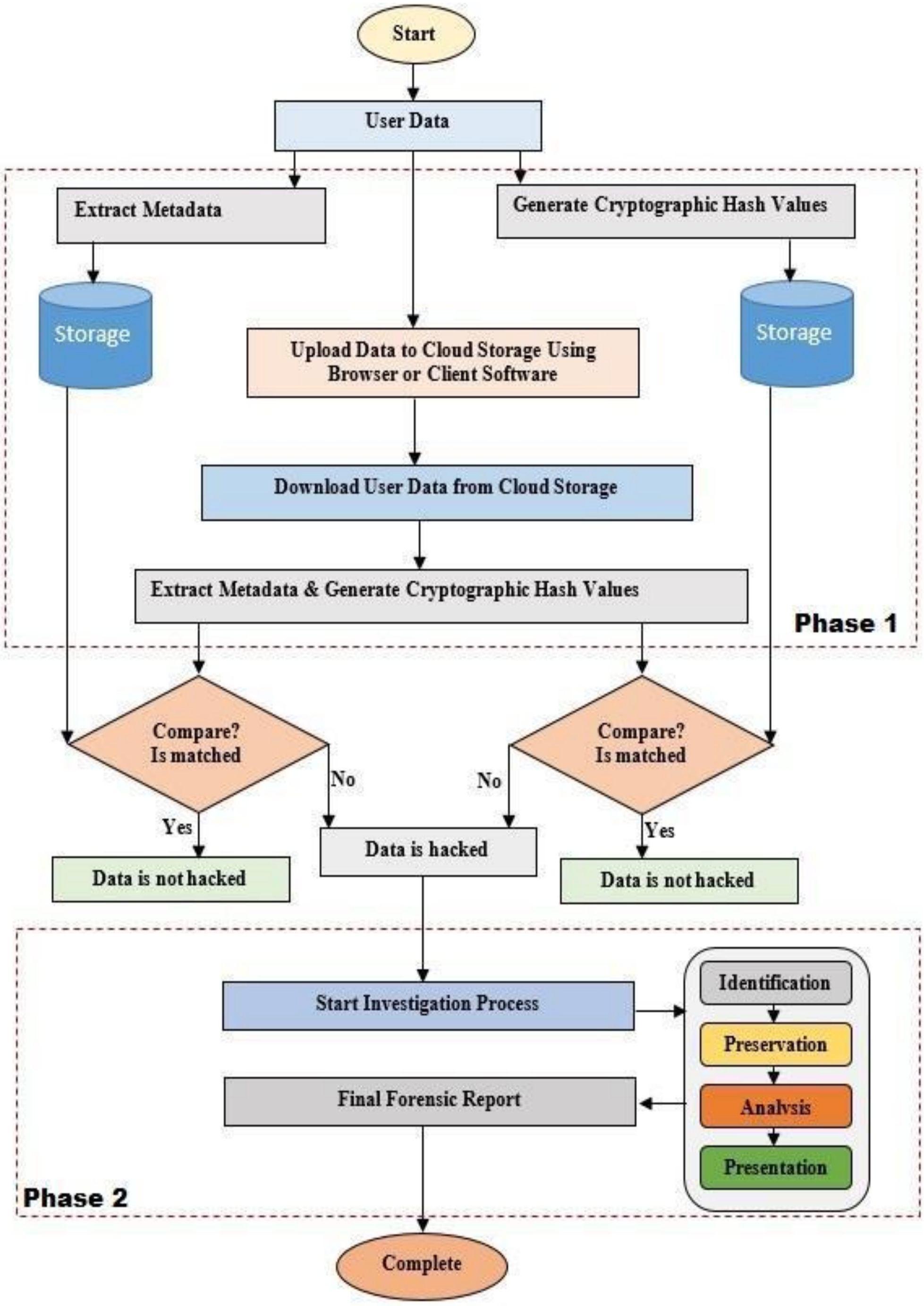


Fig.3Flowchart of Proposed Approach

Procedure of Forensic Investigation: The flowchart for performing digital investigation for cloud storage data is illustrated in Figure 4.

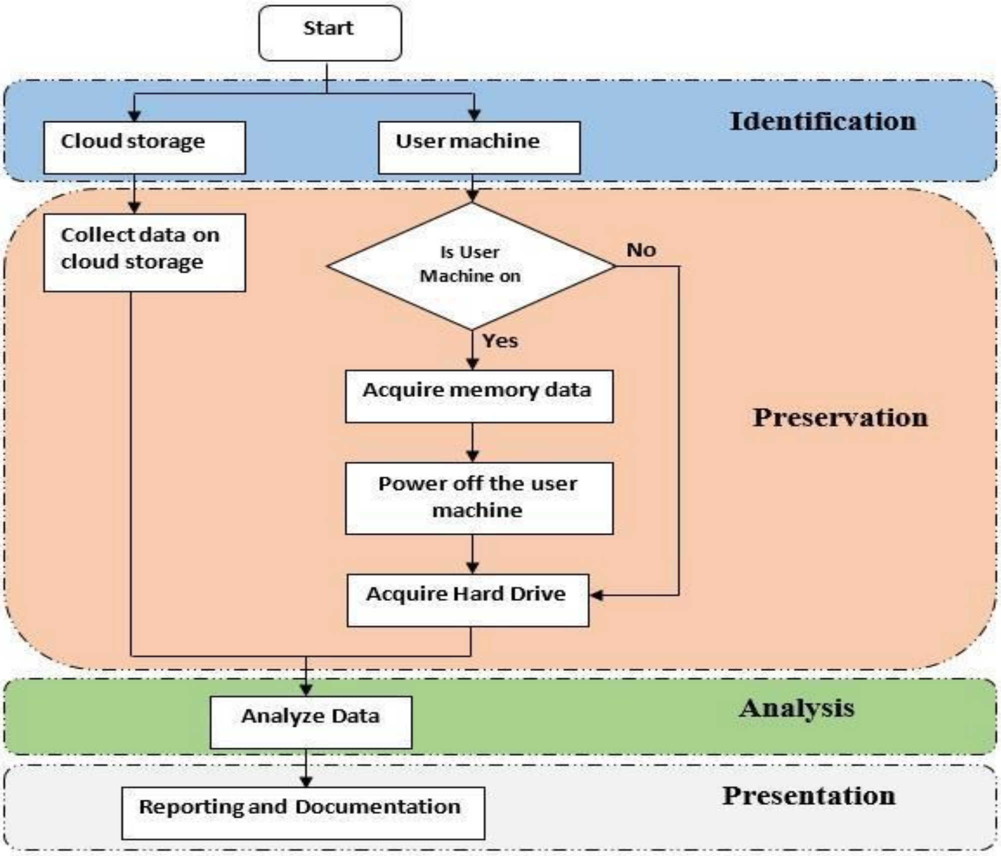


Fig.4Proposed Digital Forensic Procedure for Cloud Storage.

Digital Forensics: Digital forensics is a science to help cops and computerized examiner to distinguish, gather and break down advanced impression or proof which are gathered from a crime scene. There are four principle ventures for performing examination measure. These means involve ID, protection, examination, and show.

Recognizable proof: It is the cycle of ID of an episode and advanced proof, which will be needed to demonstrate the carried out crime.

Protection: In the safeguarding interaction, computerized agent saves the gathered advanced proof from crime scenes like hard plates, workstations, cell phones, and any connected bits of proof.

Examination: In the examination stage, computerized specialist deciphers and relates the evidential information to reach a resolution, which can demonstrate or invalidate common, or crimes.

Show: In this interaction, the advanced specialist makes a forensic report to sum up his discoveries of the criminal case. This report ought to be appropriate to present to the courtroom.

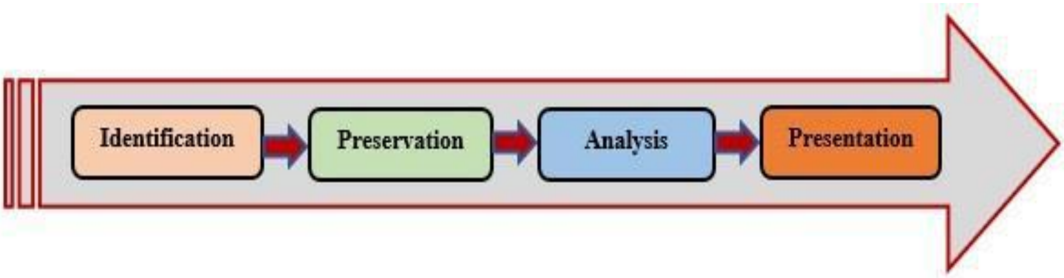


Fig.5Digital Forensic Investigation Process.

Hadoop Framework: The fundamental thought of MapReduce is to change arrangements of information to arrangements of yield information. It happens a few times that input information isn't in a lucid arrangement; it very well may be the extreme undertaking to see huge size datasets. For this situation, there is a genuine need to a model that can shape input information records into clear, justifiable yield records.

Guide Function: Map work maps stage in the MapReduce work. The guide work produces moderate yield in the equation of (key, esteem) sets. For each guide task, a new instance of the mapper is addressed in a different cycle. This capacity gets key, esteem, yield Collector, and journalist. Gather conspire from the Output Collector object onwards transitional (Key, esteem) sets to reducer as a contribution for Reduce stage.

Mix Function: Just first Map work has finished, laborers start trading halfway yield from map errands to decrease assignments. This technique for move halfway yield from the guide errands to diminish work as an info is named as rearranging. This is the single correspondence stage in MapReduce. Prior to pushing these (key, esteem) sets as a contribution to Reducers; Hadoop bunches every one of the qualities for the comparative key. Such isolated information is then designated to diminish work.

Decrease Function: Reducer example calls Reduce work for each key in the segment appointed to a Reducer. It acknowledges a key and iterator over every one of the qualities identified with that key. Diminish work likewise has boundaries, for example, iterator for all qualities, key, outputCollector, and columnist which works in a like route concerning map work.

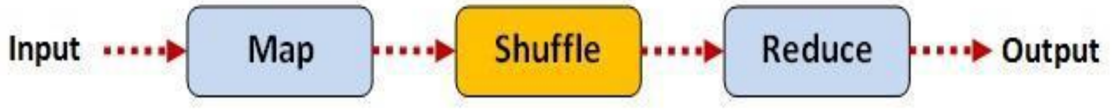


Fig.6Map Reduce Logical Data Flow.

5. Conclusion

This work worried about creating capable computerized forensic strategies for examination of cybercrimes in distributed computing climate in forensically solid and opportune way. It is presented research commitments in the field of cloud forensics. They can be summed up as follows:

A writing survey is done to investigate and recognize difficulties and openings for performing advanced forensics examination in the distributed computing climate. The ID of cloud forensic difficulties and openings, for example, secure and forensic investigation of distributed storage administrations, log information examination, plan distributed computing model to help computerized forensics, plan cloud-based forensic lab which assisted us with achieving and complete this exploration work.

A cloud forensic methodology dependent on information uprightness checking for helping and aiding computerized examiners is proposed for performing programmed advanced forensics for box distributed storage as a contextual analysis. The test results showed that there are information antiques that stay in the client machine that utilizes Windows 7 about utilizing box distributed storage, for example, IP address, and client account data like a username. The proposed approach can possibly valuable device for performing cybercrimes examination identified with cloud stockpiles.

A forensic methodology is given to examination of cybercrimes in a private cloud climate. The proposed approach can help computerized specialists and experts in securing and assortment of advanced proof from the private cloud frameworks particularly virtual machine which is viewed as the fundamental component of virtualized cloud frameworks. In increments to can gather and concentrate data from the customer gadget, hypervisor, and hypervisor the executives framework to work with the examination interaction in a viable way. Additionally, introduced a forensic strategy which can be utilized for exploring and dissecting virtual machine and its previews for aiding the reproduction of crimes which done utilizing a virtual machine.

References

[1].Fiterman, E. M., and J. D. Durick. "Ghost in the machine: Forensic evidence collection in the virtual environment." Digital Forensics Magazine 2 (2020): 73-77.

[2]. Ezz El-Din Hemdan and Manjaiah D.H," Exploring Digital Forensic Investigation Issues For Cyber Crimes In Cloud Computing Environment", Proceeding of 1st International Conference on Computer Communication and Networks (i3CN),2015.

[3]. Market Research Media, "Global cloud computing market forecast 2015-2020", http://www.marketresearchmedia.com/ ?p=839, [Accessed June 25, 2015].

[4]. Clavister, "Clavister's new dimension in network security reaches the Cloud", http://www. clavister.com/documents/resources/white-papers/ clavister-whpsecurity-in-the-cloud-gb.pdf, Clavister White Paper, [Accessed December 27, 2016].

[5]. Barrett, Diane, and Greg Kipper, "Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments", Syngress, 2010.

[6]. P. Mell and T. Grance, "The NIST definition of cloud computing" (NIST SP 800-145), National Institute of Standards and Technology, U.S. Department of Commerce, 2018.

[7]. Cloud Security Alliance [CSA], "Security guidance for critical areas of focus in cloud computing", V2.1. San Francisco, California, 2019.

[8]. DFRWS technical report, “A road map for digital forensic research”, Digital Forensic Research Workshop. G. Palmer. Utica, New York, 2001.

[9]. Mounir kamal (2012), “digital investigation concepts”, Security Kaizen Magazine, 2(6),6-10,

[10]. Keyun Ruan, Joe Carthy, Tahar Kechadi and Ibrahim Baggili, “Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results", Elsevier, Digital Investigation vol.10, pp.34–43, 2013.

[11]. NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory, “NIST cloud computing forensic science challenges” (NISTIR 8006), National Institute of Standards and Technology, U.S. Department of Commerce, 2014.

[12]. Ruan K., J. Carthy, T. Kechadi, M. Crosbie, “Cloud Forensics”, 7th IFIPAdvances in Digital Forensics VII, G. Peterson and S. Shenoi (eds), vol. 361, pp. 35-46, 2011.

[13]. Shams Zawoad, Ragib Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems", arXiv:1302.6312v1 [cs.DC], pp. 1-15, 2013.

[14]. J. Dykstra and A. Sherman, “Acquiring forensic evidence from infrastructure-as-aservice cloud computing: Exploring and evaluating tools, trust, and techniques”, DoD Cyber Crime Conference, January 2012.

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

[16]. Zafarullah, F. Anwar, and Z. Anwar, “Digital forensics for eucalyptus”, in Frontiers of Information Technology (FIT). IEEE, 2011, pp. 110–116.

[17]. D. Birk and C. Wegener, “Technical issues of forensic investigations in cloud computing environments”, Systematic Approaches to Digital Forensic Engineering, 2011.

[18]. J. Dykstra and A. Sherman, “Understanding issues in cloud forensics: Two hypothetical case studies”, Journal of Network Forensics, vol. b, no. 3, pp. 19–31, 2011.

[19]. S. Biggs and S. Vidalis, “Cloud computing: The impact on digital forensic investigations”, in In Proceedings of the International Conference for Internet Technology and Secured Transactions, ICITST. IEEE, 2009, pp. 1–6.

[20]. B. Hay and K. Nance, “Forensics examination of volatile system data using virtual introspection”, ACM SIGOPS Operating Systems Review, vol. 42, no. 3, pp. 74–82, 2018.