Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 5 – No.3, June 2016 – www.caeaccess.org

Comparitive Study of Cloud Forensics Tools

Sameena Naaz
Department of Computer Science and Engineering
Faculty of Engineering and Technology
Jamia Hamdard
New Delhi – 62, India

Faizan Ahmad Siddiqui
Department of Computer Science and Engineering
Faculty of Engineering and Technology
Jamia Hamdard
New Delhi – 62, India

ABSTRACT
In recent years, cloud computing has become popular as a cost-effective and efficient computing paradigm. Cloud computing may well become one the most transformative technologies in the history of computing. Cloud service providers and customers have yet to establish adequate forensic capabilities that could support investigations of criminal activities in the cloud [1]. It is impossible to avoid the vulnerabilities and criminal targeting of cloud environments which demands an understanding of how digital forensic investigations of the cloud can be accomplished. Unfortunately, today's cloud computing architectures are not designed for security and forensics. To date, very little research has been done to develop the theory and practice of cloud forensics. Many factors create difficulty in forensics investigations in a cloud environment.

Numerous clients stay hesitant to move their business IT base totally to the cloud. One of the primary worries of clients is Cloud security and the risk of the obscure. Cloud Service Providers (CSP) empower this observation by not giving their clients a chance to see what is behind their "Virtual shade" implies how our data or information is dealt with at the back end [2]. This paper talks about existing examination ventures and highlights the open issues and future headings in cloud crime scene investigation research territory. It has been demonstrated that the efficient methodology towards understanding the nature and difficulties of cloud crime scene investigation will permit researchers to look at conceivable secure arrangement approaches, prompting expanded trust on and reception of distributed computing, particularly in business, medicinal services, and national security. This thus will prompt lower cost and long haul advantage to the general public overall [3].

General Terms
Cloud Computing, Forensic Tools, Cyber Crime.

Keywords
Cloud computing, Digital forensics, Cloud forensics, Live forensics.

1. INTRODUCTION
Cloud computing is a quickly advancing wonder of data innovation. It can be expected as the most transformative advances ever.

Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics. Basically, it is a cross-discipline between cloud computing and digital forensics.

As per the official definition of NIST:

"Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data [4]"

Cloud forensics can likewise be considered as a subset of system legal sciences, since system crime scene investigation manages scientific examinations in any sort of system, be they private or open. Cloud computing thus, depends on expansive and broad system access, and subsequently takes after the fundamental standards found in the system measurable procedure with a few strategies exclusively custom-made for the cloud computing environment.

Cloud administration suppliers and clients need to build up some sufficient advancements and criminology abilities keeping in mind the end goal to bolster examinations of criminal exercises on cloud.

Rather than managing a physical IT infrastructure to host their software applications, organizations are moving towards the remote and virtualized environment. One of the main concern of customers is cloud security and the threat of unknown.

Cloud computing technology has shown massive game-changing potential which is exhibited by other significant computing technologies such as mainframes, PCs, minicomputers, and even smartphones. It has the ability to radically alter the way information technology services are created, accessed, and managed [5].

The number of crimes related to computers and the Internet has grown over the last decade, which in turn resulted in an equal increase in companies that want to assist law enforcement by using digital evidence to determine the perpetrators, methods, victims, and timing of computer crime. This resulted in digital forensics evolving enough to assure proper representation of cybercrime evidence data in court. However, with storage capacity outpacing network bandwidth and latency improvements, forensic data is starting to grow exponentially to the point that it makes it harder to process them in a timely manner [6].

As discussed Cloud Forensics is a cross discipline of cloud computing and digital forensics so here we need to implement the forensics mechanism to provide investigation on cloud. Cloud is a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers and these servers contain huge amount of differential data that need to be secured properly. If some kind of intrusion or false access occurs then we need some fine and fast tracking tool or mechanism so that we can perform forensics acquisition of cloud computing environment. It is not possible to perform the forensics of whole cloud area because the storage area is vast and huge and may be in

different servers at different locations. It can take infinite time for acquisition of whole cloud. We will only perform the forensics of limited area where some false action has been done or the related area. Here forensics means we will perform the analysis of cloud data so that we can find evidence against the intruder. The forensics activity will involve different types of tools and software's which can help us to perform analysis of cloud data up to some extent [7].

In this era everybody is involved in usage of internet and by its usage all are connected to the cloud in some sense or other for the purpose of saving data. This data is maintained by various data centers. But the main question that arises here is: Is our data secure at the data centers which are maintained and governed by third party? And here we are not sure about it. We are using different types of apps in mobiles like WhatsApp which contains huge amount of data that is stored at some storage place or the database of application. We are unaware about the place of storage, who has access to that data, can we trust the authorized person who has access to that data? And a lot more things come to our mind when it comes to our personal data in which our data need to be secured with some cryptographic algorithms or hash codes so that only we can access that data stored at some data center maintained by third party.

Once the problem of data storage and security has been discussed, we need to discuss the challenges that can arise in cloud environment and then how we can tackle them with forensics acquisition. In cloud forensics, the lack of physical access to servers constitutes new and disruptive challenges for investigators. Due to the decentralized nature of data processing in the cloud, traditional approaches to evidence collection and recovery are no longer practical. We need to focus on the technical aspects of digital forensics in distributed cloud environment [8]. Digital investigations have to be performed from a technical standpoint. Security policies cannot be easily employed in cloud computing environment. If some kind of security breach or incidence occurs, the corporate security team wants to be able to perform their own investigation without dependency on third parties. In the cloud this is not possible anymore. The CSP obtains all the power over the cloud environment mainly biasing the way an investigation may be processed.

In this paper forensics tools used to perform analysis on cloud have been studied and compared. The cloud forensic tools FROST and UFED physical analyzer are discussed in detail in this paper.

2. OBJECTIVE AND SCOPE

The rapid advancements and increase in popularity of cloud technology is certainly pushing digital forensics to a whole new level. Many existing challenges may be exacerbated by the cloud technology, such as various jurisdictional issues and lack of international coordination, but the environment also brings unique opportunities for foundational policies and standards.

Opportunities to be set up as an objective for cloud Forensics

- Cost Effectiveness
- Data Abundance
- Setting of Standards and Policies
- Forensics as a Service

Our primary goal depends on finding or performing legal sciences movement on cloud in the event that some sort of interruption had happened and we are unconscious about it we are simply confronting misfortune which has happened. We need appropriate devices to perform crime scene investigation examination on cloud with the goal that we can without much of a stretch catch the gatecrasher [9].

3. METHODOLOGY

It includes three dimensions

- **The Technical Dimension** – the specialized measurement includes an arrangement of apparatus and methodology expected to complete the criminological procedure in distributed computing situations. This incorporates measurable information accumulation, flexible/static/live legal sciences, proof isolation, examinations in virtualized situations, and ace dynamic arrangements.
- **The Organizational Dimension** – with regards to legal examinations in distributed computing situations, two parties are constantly included: the cloud customer and the CSP.
- **Chain of Dependencies** – The applications hosted on the cloud and the CSPs providing these services are dependent on other CSPs as well. The level of complexity on these dependencies vary and they are highly dynamic in nature. Hence any forensic investigation on any CSP or client depends upon the other CSPs which may be indirectly involved. The dependence on so many parties makes the investigation process tedious as well as difficult as there are chances that some of the parties do not cooperate or may be some of them become corrupt [9,10].

4. TOOLS FOR CLOUD FORENSICS

If some kind of falsification or intrusion is suspected in cloud first the network has to be checked by performing various steps of network forensics so as to obtain any evidence from the network.

4.1 FROST

FROST is a forensics tool for the OpenStack cloud computing platform. This tool acquires data from API logs, virtual disks and guest firewall logs in order to carry out the digital forensic investigation. FROST provides Infrastructure-as-a-Service (IaaS) cloud. This tool stores the log data in Hash trees and returns it in Cryptographic form. It works at the cloud management plane and hence does not need to interact with the operating system inside the guest virtual machines. Therefore no trust is needed in these machines.

The FROST tools are user driven so no interaction of the forensic examiners and customers with the Cloud service providers are needed for law enforcement. The latest features of these tools allow forensic experts to extract the required forensic data from the OpenStack cloud without the provider's interaction.

The outline has an extensible arrangement of scientific goals, including the future expansion of other information safeguarding methods, revelation techniques, checking procedures, measurements and reviewing abilities.

Hence, clients of open cloud administrations do not require the help of their cloud supplier for any forensic examination. Law authorization depends on the bulky and tedious court order procedure to acquire cloud information, and requires the cloud supplier to execute every inquiry in the interest of the requester. In [11] it has been reasoned that the administration plane is an alluring answer for client driven scientific abilities since it gives access to criminological information without expecting to believe the visitor virtual machine (VM) or the hypervisor, and without requiring help from the cloud supplier. Putting away and getting reliable proof from an outsider supplier is non-paltry.

Its commitments are-

- Description of the engineering, outline objectives, and execution of client driven measurable obtaining of API logs, virtual disks, and firewall logs from the administration plane of Open Stack.
- A calculation for putting away and recovering log information with uprightness in a hash tree that coherently isolates the information of every cloud client in his or her own particular sub tree.
- Evaluation results demonstrating that the proposed arrangement fulfills mechanical and lawful prerequisites for acknowledgment in court and scales properly for a cloud environment.

4.1.1 Requirements, Specifications, and Capabilities

This tool can be used by different stakeholders for different purposes. It satisfies the forensic community and legal requirements as well. There could be two categories of stakeholders who are using this tool for solving Cloud forensic issues.

One is a person committing crime against an innocent victim who is ready to cooperate. This victim could have had any type of resource on the cloud which has been compromised. The FROST tool could be deployed either at the innocent victims end or can be used by the law enforcement body to deal with such crimes. Another type of crime is the one which has been committed by a non-cooperative party where cloud has been used as an instrument of crime. In this situation the tool could either be at the law enforcement end or it could be deployed at the cloud service provider's end. Any ways in both the situations interaction with the people working at the provider end is minimal as the work has been automated using the FROST tool.

The technical requirements of the tool has to be in accordance with the cloud environment. Some of the characteristics of the cloud are self-service, on demand, scalability and elasticity. The tool being developed should be compatible with all these characteristics. The technical specifications that fulfil these characteristics are:

1. Compatibility with existing forensic formats.
2. Easy to generate
3. Extensible and open
4. Scalable
5. In accordance with existing and standards

The three main components of FROST and their functions are:

1. The image of the virtual disk of any user's virtual machine can be retrieved using this tool and then the integrity of these images can be validated using cryptographic checksums.
2. Logs of all the API requests to the cloud provider made by a user using his/her own credentials can be retrieved by him/her and their integrity can be validated.
3. OpenStack firewall logs for any of the user's virtual machines can be retrieved and it's integrity validated using this tool.

4.1.2 Architecture and Features

OpenStack has numerous segments, however two have been incorporated in FROST: Nova and Horizon. In Nova the compute service is provided through the virtual servers as in Amazon EC2 and the compute API is implemented. Web based user interface for OpenStack is provided by Horizon and it communicates with Nova through Compute API. Figure 1 shows the integration of Nova and Horizon with OpenStack.[12]

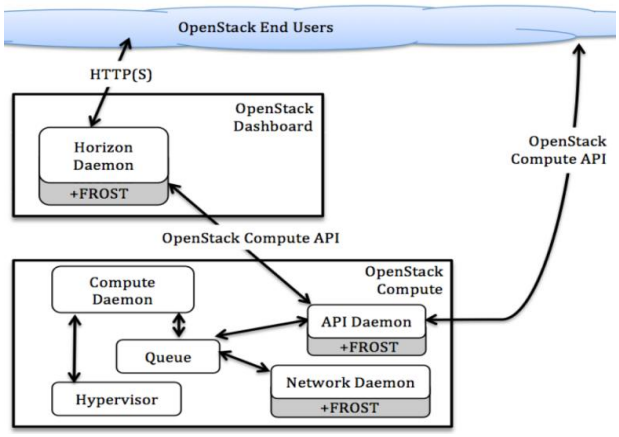

Figure 1: **Open Stack architecture showing where Open Stack Compute (Nova) and Open Stack Dashboard (Horizon) have been modified to add FROST.**

So we can say that FROST suite for OpenStack is a collection of forensic tools which is integrated into the management plane of a cloud architecture. These tools can be used by law enforcement, cloud consumers, law enforcement and forensic investigators for acquiring trustworthy forensic data independent of the cloud provider. This tool can also be used for metrics, real-time monitoring or auditing. User accessible concrete capabilities are offered by FROST.

While numerous organizations are still reluctant to embrace cloud arrangements in light of security concerns, FROST arms them with capable and quick reaction capacities. All commercial cloud services should be using these types of tools so that the cloud forensic problems can be solved. [12, 13].

4.2 UFED Cloud Analyzer

Forensic investigators get huge amount of potential evidence for their investigations from the cloud information sources. Hence these sources act as virtual goldmine of very valuable

data. Data from mobile devices can be captured using various tools and can be used by investigators to solve crimes related to the cyber world. The cloud service providers want to maintain the confidentiality of their clients, so they use various mechanisms to ensure that the data cannot be captured by anyone else. Hence accessing this data for criminal investigations always remains a challenge. Data from private social media accounts such as Facebook, Twitter, Kik and Instagram can be extracted, preserved and analyzed using The UFED Cloud Analyzer tool being discussed here. It also provides for file storage and other means of speeding up investigations.

Existing cloud data as well as metadata can be collected using UFED PRO Series and can be packaged in a manner which can very easily be used for forensic examination. This tool has efficient searching as well as filtering and sorting capability which provides very important details about "Who? When? Where?" has committed any crime which can help the experts move in the correct direction during investigation. [14].

4.2.1 Key Features of UFED Cloud Analyzer

Extraction based upon mobile device

Login information extracted from the mobile device is used to access private-user cloud data.

Extraction based upon username

Usernames and passwords provided by the investigated subject or retrieved from personal files and contacts or via other discovery means is used to login to private-user cloud data.

Preservation of forensic data

The entire process of data extraction from the cloud is traced by logging in to maintain data authenticity. Each piece of extracted data is hashed separately and can be later compared against its origin.

Unified format is used to visualize the data

Different cloud services are normalized in a unified format and can be viewed in Timeline, File Thumbnails, Contacts or Maps format.

Data can be reported, shared & exported

This tool can generate and share easy-to read, PDF reports for entire data sets or filtered Information. Extracted data can be exported to other analytical tools for deeper analysis and Cross source investigation with third party data.

4.2.2 Timely Extractions of Private User Data can be performed

Login credentials extracted from a mobile device can be used by examiners to extract private user cloud data from various social media, webmail and cloud storage sources without going outside the legal boundaries. This tool comes as a very useful instrument especially in cases where the service provider is not cooperative. Using this tool the forensic experts can access authentic data at a fast speed.

4.2.3 Different Types of Data can be Unified and Organized into a Common View

Large cloud data sets can be dynamically visualized and analyzed in a unified format so that the analysis and comparison becomes easy. The disparate data retrieved from various service providers can be normalized and organized into a uniform format which helps the forensic experts to look at the common connections and correlate critical evidences. Immediate access to private cloud data helps in saving valuable time as that this data can be compared with the data provided by the service provider and any manipulations by the provider can be checked at an early stage.

4.2.4 Data can be Shared and Integrated for Further Analysis

UFED has made sharing of various evidences and other information among the people working on a case easier. The supervisors, command leaders attorneys and other outside parties can use this tool to share their investigation results. The data that they receive using this tool is comprehensive, relevant and mission specific. The UFED Cloud Analyzer data can be easily integrated with UFED Link Analysis also for deeper analysis.

4.2.5 The Investigative workflow is simplified by the UFED Cloud Analyzer

The steps involved in using the UFED Cloud Analyzer for any forensic investigation are as listed below:

1. Mobile device is seized from the perspective criminal.
2. UFED Physical Analyzer is used to decode cloud services login information.
3. Login information or credentials is used to extract private user data.
4. Data is analyzed and reported in a unified format.
5. Data is shared and the investigation proceeds further using UFED link Analyzer or other analytical tools.

5. UFED CLOUD ANALYZER BASICS

UFED Cloud Analyzer is a Windows based extraction and analysis software which is designed to import a file that contains account credentials from popular cloud services. This extraction can be carried out from UFED physical analyzer using either a file system or by physical extraction of a smartphone's memory. Usernames and passwords can also be manually entered by the investigators. Then the service provider's application programming interface (API) is used by the UFED Cloud Analyzer to collect "snapshots" of private cloud-based evidence.

Some of the best practices for scientific cloud extraction which the UFED Cloud Analyzer clients should adhere to are:

- The Cloud Service provider should be given proper legal notices and all the rules for the examiner's country should be followed properly.
- Special storage media has to be used for forensic data which is extracted. This may be an external drive, a flash drive, a location on an internal forensic network, an internal drive or a partition within the forensic computer.

The system requirements for UFED Cloud Analyzer are:

- PC: Windows Compatible PC with a dual core or compatible processor running at 1.6 GHz or higher
- Memory: Minimum - 8 GB

- Operating System: Windows 7 Service Pack 1, Windows 8, 64 – bit or Windows 10, 64 – bit.
- Space: 90 MB of free disk space for installation
- Microsoft.Net Framework version 4.5.2

6. SPEEDING CLOUD DATA EXTRACTIONS REMOTELY

As a major aspect of the UFED Pro Series and the principal measurable instrument of its kind, UFED Cloud Analyzer conveys auspicious access, conservation and investigation of online networking information. Inside preapproved legitimate limits, it empowers inspectors and specialists to gather both existing cloud information and metadata without record certifications. UFED Cloud Analyzer copies the client's accreditations put away inside the gadget to perform the remote accumulation and after that bundles the information in a forensically solid way. Clients can without much of a stretch hunt, channel and sort information to rapidly distinguish key points of interest and uncover basic proof that can eventually build up guiltlessness or blame.

This Tool Allows Users To:

- Access private-client cloud information using login data extricated from the cell phone or by utilizing usernames and passwords gave by the subject, recovered from individual documents, contacts or by means of other revelation implies.
- Extract data from cloud information sources including Facebook, Twitter, Gmail, Drop box and other information sources while logging and following the whole procedure to keep up information realness .
- Extract detailed location information from a suspect's or casualty's private Google Location History put away on Google cloud servers, permitting examiners to track time stamped developments minute by moment.
- Track and break down a suspect's Facebook Likes and Events and Twitter presents and associations on show signs of improvement comprehension of a suspect or casualty's interests, connections, assessments and day by day exercises.
- Normalize dissimilar information into a brought together arrangement and progressively picture different information sources in Timeline, File Thumbnails, Contacts or Maps group for simpler examination.

6.1 Solving Cloud Extraction Problems with an Account Based Approach

As the amount of data in a cloud environment is very huge, so finding out the exact evidence is very difficult. The UFED Cloud analyzer extracts data from the user's mobile device. Likely sources of evidences can be identified from this data.

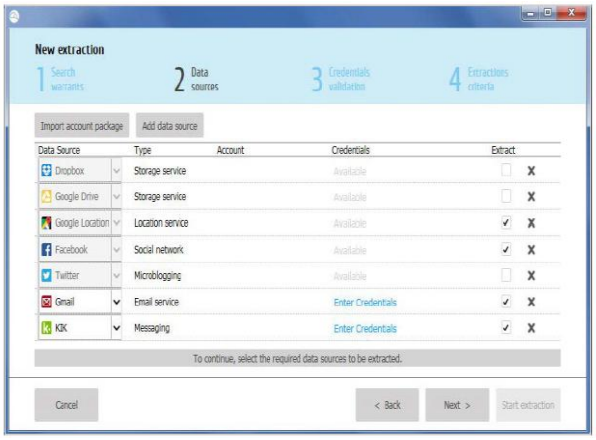

Figure 2: Sample data extracted from user's mobile device

Once an evidence has been identified by an investigator imaging of cloud may be needed although it is difficult due to high volumes of evidence and location issues. Another problem is that data may be scattered on various servers and may be mixed among data pieces belonging to other accounts. This makes the computer forensics concept of "imaging" a hard drive impractical, and probably not applicable for the realm of cloud-stored data.

UFED Cloud Analyzer's record based methodology diminishes these dangers by concentrating on a particular client's information, regardless of where it's stored. NIST recognizes that this specific information securing is a test on the grounds that earlier learning about important information sources is often hard to get in a cloud environment.

6.2 Solving forensic cloud storage problems using Service provider's APIs

UFED Cloud Analyzer relies upon the service provider's API to extract data. If the API allows, an investigator can access deleted or archived data. However, along with identifying data via hash value, the use of account credentials means that UFED Cloud Analyzer does allow data - deleted or live - to be attributed to a specific user.

7. CLOUD FORENSICS CHALLENGES

Undoubtedly, a few difficulties remain and will require progressing dialog.

These include:

- Finding out the source of an unauthorized change to the cloud computing environment of a client.
- There could be some jurisdictional issues which may arise due to different location of the people involved that can influence the chain of guardianship. NIST talks about various individuals who may be involved with protecting and gathering information present on physical hard drives in different areas. Whether this makes any difference in the court of law or not is still debatable.
- The Cloud's operational details and Cloud Service Provider's API are not very transparent and this also hinders the forensic investigations.

- There may be criminal organizations which work independently and may be involved, but it may be difficult to nail them as their association with the crime is difficult to prove due to the distributed nature of the cloud computing environment.
- It is difficult to judge that which logs can be used as evidence is case of any crime and hence there is an uncertainty on what has to be logged and what not.
- Worldwide cloud administrations, and how law implementation can guarantee it is getting lawful access to information in a way that is not as of now clear.
- Absence of standard computerized criminological procedures and models, including standard systems and best practices for examinations in the cloud.
- Not knowing where information is put away or who has entry to it makes it more difficult to survey whether confirmation was spilled or defiled and consequently, whether agents kept up chain of authority. The certification based extraction procedure is a beginning, yet not a panacea. In spite of the fact that UFED Cloud Analyzer forestalls different logins while an examiner is utilizing the product, this doesn't control for record movement before or after investigative login [16].

8. COMPARISON OF FROST AND UFED

FROST	**UFED Cloud Analyzer**
FROST is incorporated with open stack and first to be incorporated with Infrastructure- as- a- Service (IAAS) cloud platform.	UFED cloud analyzer is a tool for cloud data extraction, analysis, conservation and investigation of online networking accounts and drives.
In FROST the cloud client can recover the virtual disk from any client site or virtual machine and approves it with cryptographic checksum.	UFED pro series is an intense investigating tool which can collect both cloud data and metadata in a forensically solid way. Analyst can enquiry information of who? when? why?
Logs of all the API requests to the cloud provider made by a user using his/her own credentials can be retrieved by him/her and their integrity can be validated.	This approach adequately protects the security of different inhabitants gathered on the same server, and minimizes issues with confirmation being scattered around various storage areas.
The cloud client can recover the OpenStack firewall logs for any of the client's virtual machines, and approve the integrity of those logs.	A Cloud Analyzer extraction hashes every individual antiquity and, independently, its related metadata.
The proposed solution assumes a trusted cloud provider and cloud infrastructure.	The cloud provider may or may not be a trusted entity.
Cloud clients associate with their supplier and oversee cloud assets through the administration plane utilizing a web interface and API.	Cloud Analyzer utilizes the supplier's application programming interface (API) to gather "depictions" of private cloud-based proof.
Example: Consider a subjective cloud client Alice who needs to examine suspiciously high transmission capacity utilization from her cloud-facilitated webserver. Besides the logging of web demands that she does within her own particular VM, Alice would have a more finish picture of action on the off chance that she could likewise get a record of administration movement and metadata about her VMs. Our answer gathers and gives reliable API logs, visitor firewall logs, and virtual plates. These information can build a timetable of action and comprehend an episode.	Example: Accepting the agent has the mobile device or can rapidly distinguish a suspect, the mobile device can affirm a suspect's actual character and record ownership. As it were, utilizing a suspect's mobile device to get login certifications implies that examiners are in a superior position to validate the confirmation. UFED Cloud Analyzer depends upon the administration supplier's API to concentrate information. In the event that the API permits, an agent can get to erased or documented information.

9. CONCLUSION

The need for forensics in cloud comes if any unauthorized access is done on cloud which is having lots of confidential data. We are just using cloud for storing large amount of data and of being unaware about the security and privacy of data, not knowing anything about back end. It is very much needed to know about the data Centre where we are storing data and to know how secure our data is.

The fast progressions and expansion in prominence of cloud innovation is absolutely pushing advanced legal sciences to a radical new level. Numerous current difficulties might be exacerbated by the cloud innovation, for example, different jurisdictional issues and absence of global coordination, however the earth likewise brings novel open doors for foundational arrangements and measures. The cloud is both another front line for cybercrime, and additionally another reproducing ground for novel investigative methodologies.

Much like any new innovation and region of exploration, there is much to be done and each information in this archive only focuses individuals towards the correct heading.

There is additionally the requirement for legitimate issues in regards to mists including information maintenance and protection laws to be reevaluated, taking after the far reaching reception of cloud advances. At last, there is likewise the requirement for the computerized crime scene investigation group to start setting up standard experimental components to assess structures, techniques and programming instruments for use in a cloud situation. Just when examination has been directed to demonstrate the genuine effect of the cloud on advanced legal sciences, would we be able to make sure how to modify and create elective structures and rules and also apparatuses to battle digital wrong doing in the cloud.

As talked about in past segments flow issues in the range of cloud legal sciences examinations bolster the advancement of a quick research plan in the region of techniques, instruments, philosophies, and particular situations. These issues will be of worry to both the general population and private segments. This segment particularly analyzes a few zones of examination that the creators expect to direct to assist comprehend computerized legal sciences examinations in the cloud that include: an examination of cloud administration utilization, the adequacy of procurement strategies, a comprehension of business cloud situations, an examination of cloud measurable administration, and the effect of the cloud on cell phones[1,2,9,16].

10. REFERENCES

[1] Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, "CLOUD FORENSICS," Advances in Digital Forensics VII, IFIP AICT 361, pp. 35–46, 2011. IFIP International Federation for Information Processing 2011.

[2] Dominik Birk, "Technical Challenges of Forensic Investigations in Cloud Computing Environment" January 12, 2011.

[3] Shams Zawoad, Ragib Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," University of Alabama at Birmingham ISSN-35294-1170 March 2014.

[4] Willie E. May, "NIST Cloud Computing Forensic Science Challenges" National Institute of Standards and Technology Interagency or Internal Report 8006 (June 2014).

[5] Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, "Cloud_Forensics: An Overview", Advances in Digital Forensics VII, IFIP International Federation for Information Processing 2011.

[6] Vladimir Dobrosavljević, Mladen Veinović, Ivan Barać, "Standard Implementation in Cloud Forensics" Singidunum University, Danijelova 32, Belgrade, Serbia 2015.

[7] Dorey P.G., Leite A, "Commentary: Cloud computing – A security problem or solution?" Information Security Technical Report, 16 (3–4), pp. 89–96, Elsevier (2011)

[8] S. D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments," Fifth International Conference on IT Security Incident Management and IT Forensics,pp. 3-9, 2009.

[9] Xath Cruz**,** "The Basics of Cloud Forensics," cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/Nov 2012.

[10] Yunting Lei, Yuyin Cui, "Research on Live Forensics in Cloud Environment" The Third Research Institute of Ministry of Public Security Shanghai, China. (3CA 2013).

[11] Dykstra J, Sherman AT, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques" Digital Investigation 2012, (Suppl. S90–S98). The Proceedings of the Twelfth Annual DFRWS Conference.

[12] Josiah Dykstra and Alan T. Sherman, "Design and Implementation of FROST: Digital Forensic Tools for the OpenStack Cloud Computing Platform," Cyber Defense Lab, Department of CSEE University of Maryland, Baltimore County (UMBC), April 2013.

[13] Josiah Dykstra and Alan T. Sherman, "Understanding Issues In Cloud Forensics: Two Hypothetical Case Studies," ADFSL Conference on Digital Forensics, Security and Law, 2011.

[14] Cellebrite, "Extracting Legally Defensible Evidence From The Cloud," Explaining UFED Cloud Analyzer Extraction and Analysis Processes.

[15] Cellebrite, "UFED Cloud Analyser" UFED-Cloud-Analyzer-DataSheet.pdf www.**cellebrite**.com/Mobile-Forensics/Products/**ufed-cloud-analyzer**

[16] Europe Proceedings of the Third Annual DFRWS Europe Forensic analysis of cloud-native artifacts Vassil Roussev, Shane McCulley. DFRWS 2016.