CLOUD FORENSIC FRAMEWORKS, CHALLENGES, STATE OF ART AND FUTURE DIRECTIONS

[1]Gayatri S Pandi , [2]Dr. K.H.Wandra,
[1]Ph.D Scholar, [2]Director,
[1]Technology of Computer Engineering,
[1]C U Shah University, Wadhwan, India

Abstract: ***Cloud Forensics is a blend of a couple of disciplines like Cloud computing and Digital Forensics. Cloud Forensics is defined as the "science of conserving all potential evidences, safeguarding the privacy and integrity of the information, identification, collection, organization, presentation, and verification of evidence data to determine the facts about an incident in the concerned cloud environment". The aims of Cloud Forensics techniques is to excerpt information for solutions of the 8Ws (Who, Why, Where, What, Which, Whom, Whose and When) from the data mined from the evidences obtained from the Cloud Forensics Logs. This paper emphases on the challenges observed in the frameworks, the state of art and future directions in the domain of cloud forensics. It analytically reviews the forensics architectures in the cloud environment prevailing challenges and resolutions, and it ascertains, entirely the effort that has been accepted in cloud forensic domain which would be of great help in examination of the security breaches in Cloud based Architectures. Additionally, the detailed assessment reveals benefits and shortcomings of the prevailing approaches providing some innovative imminent exploration guidelines and also supporting a brief discussion on Indian Cyber Laws. To sum up, this detailed review paper can be an initial point for the scholars desiring to build forensics related services that can operate on Cloud***

IndexTerms - Cloud Forensics, NIST, Cloud Computing, Digital Investigation, Digital Forensics.

I. INTRODUCTION

Forensics techniques are the measures applied to retrieve the electronic evidence data for the crime committed by the convicts. Cloud Forensics is a blend of a couple of disciplines like Cloud Computing and Digital Forensics. Cloud Forensics is defined as the "science of conserving all potential evidences, safeguarding the privacy and integrity of the information, identification, collection, organization, presentation, and verification of evidence data to determine the facts about an incident in the concerned cloud environment" [15]. The aims of Cloud Forensics techniques is to excerpt information for the solutions of the 8Ws (Who, Why, Where, What, Which, Whom, Whose and When) from the data mined from the evidences obtained from the Cloud Forensics Logs. Digital Forensics science is a division of forensic science including the retrieval and examination of traces in digital devices, which are used commit a crime using a computer or a mobile. As the Cloud has a Black Box nature, many assumptions of digital forensics become invalid in clouds [1].

II. CATEGORIES OF DIGITAL FORENSICS

Digital Forensics can be categorized as follows:
(1) Computer Forensics – defined as the methods of finding, safeguarding, collection, analysis and reporting on evidences identified on any type of computer and storage media which would be of major help during the examinations and legitimate measures.

(2)Network Forensics – defined as the process of checking, analyzing and investigating of the activities executed in the network or events in order to locate the origin of attacks, source of instructions or any other problematic happenings like malware attacks, abnormal network traffic, virus or any security breaches. Network investigations deal with volatile and dynamic information.

(3)Mobile Devices Forensics – defined as the process of gathering the evidences which are stored after committing a crime are recovered from mobile phones, smartphones, Subscriber Identity Module (SIM) cards, Personal Digital Assistant (PDA), Global Positioning Systems (GPS) devices, tablets etc.

(4)Digital Image Forensics – defined as the process in which the extraction analysis and investigation of photographic images taken from any digital device and analyze the authenticity of such images and provide its analysis.

(5)Digital Audio Forensics- defined as the process in which the acquirement, analysis and evaluation of sound recordings that can be presented as admissible evidence in the Lawful procedure of the court authority.
(6)Video Forensics – defined as the process of studying, gathering, and assessing of video recordings. The main motive is the check the genuineness of a recoding as to whether a footage is original or its maligned. The original footage can be modified either intentionally or it could have happened by an accident.

(7)Live (Memory) Forensics – defined as the process of recovering the evidence from the Primary Memory (RAM) of a powered computer, also called Live acquisition. The objective of Live acquisition is to gather the traces from systems using diverse operations and techniques applied to primary memory content. Its a very big challenge to collect traces during investigations while its Live. Tools employed is this category are Fastdump from HBGary, Memoryze from Mandiant, and FTK Imager from Access-Data.

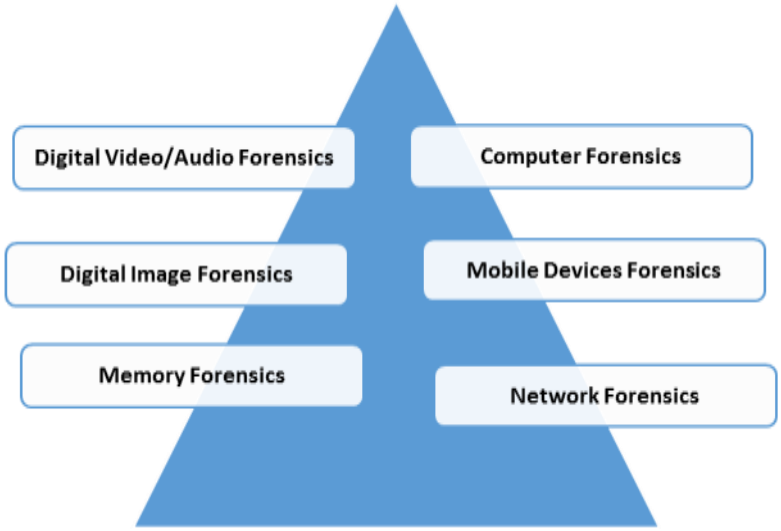

FIGURE 1: CATEGORIES OF DIGITAL FORENSICS

Some of the free tools to perform the Digital Forensic Investigation are Sans Fits, ProDiscover Basics, Sleuth Kit, FTK Imager, Caine, Oxygen Forensic Suite 2013 Standard, Bulk Extractor DEFT, Xplico, LastActivity View, and HxD [69].

III. CLOUD FORENSICS INVESTIGATING PROCESS

The investigation process is initiated whenever an incident takes place as shown in Figure [2] Step 1 as Incident.. The incident happens because when a person who wants to perform some malicious actions and can be called as a malicious user. Once such incident happens it is traced by the employees employed by the company dedicatedly for Security or by different agents employed on related cases or even by common people as show in Figure [2] as Identification.

Once the incident happens and is reported, a special group is formed which traces the breaches and tries to resolve it. The special group members are the skilled and trained persons, in the Digital security field, forensics, safety and the procedures of Law. The group is stated as Special Task Force (STF). STF's major priority is to focus on the happened incident, find solutions to it and help to sue the malicious users. As the data stays distributed in the cloud domains it becomes very grim to segregate the potential traces obtained in data centers, located at different geographical sites. Cloud Service Providers (CSPs) are presenting the unlawful data/posts in the Data Centers owned by them. Their co-operation with STF is best needed to give them access to the data, so they can segregate the cause of the issues traced and identify the evidences [2].

As the identification process stage progresses, all the people belonging to both STF and CSPs) should be proficient enough to manage with the potential evidence with extra special care. These points are shown in Step 1 Figure [2].The intention of extra special care needed here is to preserve integrity, validity and preserve the chain of custody of the evidences' traced. Data may exist in in diverse jurisdictions; STFs need to address this and a warrant from the concerned authorities should be obtained in order to get the evidence.

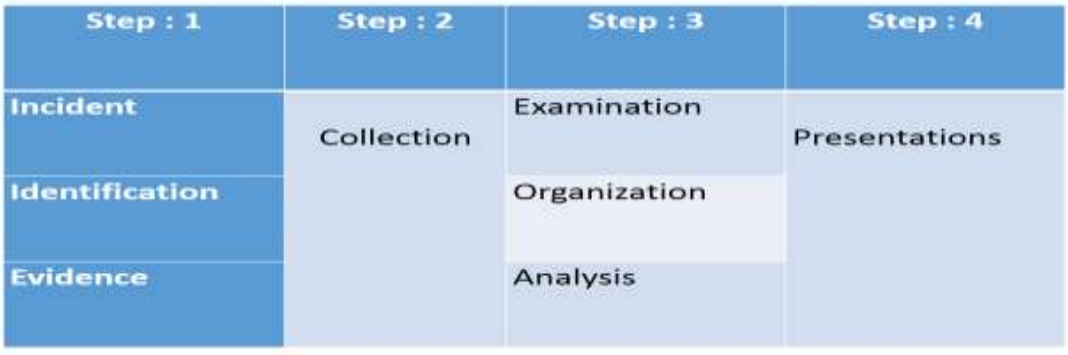

FIGURE 2: CLOUD FORENSICS PROCESS

After tracing the sources of the happened incident, skilled experts must find an appropriate way to assemble the evidences traced and protect the integrity of it. The CSPs may not appreciate the control of their infrastructures in the hands of the investigators or they may be operating in different countries, so the CSP's allocate an employee in the process of such data collections. Gathering the potential traces is a tough effort, especially in cloud environment. A lot of expertise is needed to fetch the data and a lot many variety of tools are also needed to fetch the data from various media. The sources of evidence are the software, hardware etc. termed as the assets or possessions need to be collected and examined thoroughly to produce the traces. The forensic principles are applied for the data collection process. The other clients leasing and who are allocated same data centers with the malicious users who are also the clients should be least affected by the investigation process. Also an extra effort is needed to sustain the privacy and confidentiality of such clients.

.

The process of collection of the data needs the concentration on specific leased client. Resources and Possessions collected should be documented as per the processes defined to produce an effective report. Subsequent step to be executed in the forensic process in cloud environment is the inspection of the possible evidence as shown in Step 3 Figure [2]. The traces need to be examined from these Possessions

with proper forensics tools. It should even reveal the smallest worthwhile information so that they are employed as evidence in the court of law. While examining the possessions the group may conclude that the cryptosystems using complex algorithms are employed on the data on the possessions. Experienced and well-trained personnel are needed to revel the decoded keys. At times there are situations where the data needs to be reconstructed using the varied timestamps and other significant data which can be obtained from the Analysis stage. Measures need to be very evidently defined and document the recommended finest available explanation related to the incident that has occurred. Finally to conclude the investigation process should lead to the outcome of effective reports. The study focus of the report is to abide by the procedures of law and present the same in the court of law or may be corporate management. The analysis of the traces gathered need to be converted into reports as shown in Step 4 Figure 2. The consequence of the case completely relies on how effective the reports are created and represented. So in crucial cases the experts need to be chosen who poses sufficient knowledge of the Law Procedures who have produced effective records, who have contributed in or have experience in handling such events. The Jury may lack the working knowledge of cloud computing, so the experts need to represent the collected reports in a way that Jury comprehends. The Legal Reports needs to be presented by experts who have acquired skills and expertise of the law issues and/or accompanied by a good technical background.

The evidence verification process is very significant and it needs to be preserved. As the nature of cloud data is very volatile and there is a possibility that the CSP's manipulate the evidences termed as malicious Cloud Service Providers, such steps are justifiable to be included. The data gathered for the Preservation stage must be operational always and has to be connected and must be available always due to which such processes are termed as "Continuous Forensics". It is very mandatory that the verification of the cloud based evidence is done thoroughly. This stage is termed as Verification stage .The verifier will employ the information collected during preservation stage to resolve the issues of integrity of the evidence. The evidence is worth the trust or not completely dependent on how competently and securely such data is preserved.

IV. CLOUD FORENSICS' FRAMEWORK

McKemmish et al [64] defined a framework in 1999 as shown in the Table [1]. NIST framework was defined by Kent al in 2006 as shown in the Table [1]. Ben at al have also [64] proposed a variation of the steps in the framework as presented in Table [1].

TABLE 1: CLOUD FORENSICS' FRAMEWORK COMPARISON

Ben Martini Framework (2012) (Iterative Process)	NIST Framework (Kent et al) (2006)	McKemmish et al (1999)
1. Evidence Source Identification and Preservation	1.Collection	1.Identification
2. Collection	2.Examination	2.Preservation
3. Examination and Analysis	3.Analysis	3.Analysis
4. Reporting and Presentation	4.Reporting	4.Presentation

The detailed discussion on these steps was done in the above Section III.
Table 1 Table Type Styles

V.FORENSICS SUPPORTED CLOUD ENVIRONMENT

Many Researchers have focused on building a Cloud enabled Forensics or at least a support system for Cloud Forensics. Some early researchers also worked on securing the network connections and the VMs also. Many current challenges are also listed in the documentation of NIST [65]. Corrado et al designed a framework AlmaNebula for forensic framework for cloud termed as "Forensics-as-a-Service" [9]. Srivastava et al designed a tamper resistant system for maligned network connections [27]. Payne et al[28] worked on securing and monitoring the VMs.

Flogger a term coined by Ryan Keyun L et al [24] [32]. They made many key observations that a distinct forensics architecture related to a cloud computing environment is desirable. The researchers also stated that they could employ the investigating tools found during their phase and can be extended if needed for Cloud. A "File-centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments"[32] was a new centrally defined "File-Centric Logger" apt for the private and public Cloud environments which registers the access of all the files and is also responsible for transmission of metadata from inside the kernel spaces of the VMs and physical machines (PMs) in the Cloud, thus giving entire background details in the Cloud. The Services useful for the CSP, End Users and other related users are built on top of the Cloud. The techniques used here help the system administrator and End users in assessment of Life cycle of the files and their transfer histories. The techniques also help to identify the duplicate files, tracking the malicious activities and supporting forensics. The Management API is employed to provide all the needed logs and reports.

FROST (Forensic Open Stack Tools) is built into Open Stack Cloud and as per the researchers Dykstra and Sherman [14] the first one to be built into any Infrastructure-as-a-Service (IaaS) cloud platform. FROST accumulates data at the CSP level, at the host OS level beneath the guest VMs, and assists in gathering such data within the management plane of Open Stack. A browser is used to control the virtual instances in the Open Stack Cloud. The investigators can collect the forensics data without interacting with the virtual machines. Hence the forensics data collected is sealed from a conceded or un-reliable virtual instances. The Open Stack cloud has several key components like Nova, Horizon and many others. FROST interacts with Nova which provides the computer service through virtual servers and implements the computer API. The other component it interacts with is the Horizon which offers the GUI for the users applicable on the web for OpenStack. FROST does not provide the entire picture of all the happenings of the Cloud environment. Although the Compute Node provides the different types of logs like the audit logs, firewall logs and instance and virtual instance information, the packet information can be captured through the Network and the Controller Node. The Management plane is weak and can be the target of assaults. An intelligent malicious user can break through the system with entry points from the dashboard or the Management plane can also drudge the "FROST framework". The forensics activities can be performed by the Users from the Management plane, but this is the point where a security breach occurs. Such activates through the management plane is not always appreciated due to certain flaws. Some intermediary and self-governing level which interminglies with physical level is additionally needed to capture and analyze the cloud environment. Also, an attacker intending to meddle

with other user's accounts can governor the FROST interface by himself to be left with no evidence about his activities. J. Dykstra et al [14] also mentioned that the management console and the APIS needs an added level of trust. The researchers never referred to any scheme for persistent storage of logs and making these logs publicly available.

Sean Thorpe et al [10] [16] [30] [33], have referred to numerous service delivery prototypes in cloud. The researchers also defined the transitional cloud brokers with diverse SLA agreements [34] [35]. A framework for Forensics was projected by N H Ab et al. [40] for "Cyber-Physical Cloud Systems (CPCS)". This conceptual framework emphasized the significance of forensic readiness and covers many factors. It guarantees that a CPCS is aimed to aid in the investigations involving the crimes. The "forensic-by-design" approach can provision the digital investigation process by recognizing and shaping the origin of evidence and by speed up the investigation process. Aydin et al have debated about concerns in the forensics of cloud domain like the confidentiality, performance and network overhead and integrity [72]. Here the authors have dealt with confidentiality issues in procurement of instances images and its integrity together for object and block storage and their verification. Sato et al replaced a library in the VMS for the securing them [36]. Chen et al [39] provided suggestions for digital forensics in cloud domain. Mishra et al [46] explained about the state-of-art and research challenges in cloud domain. Harberlen et al [47] discussed about a case for an accountable cloud.

VI.CHALLENGES WITNESSED IN CLOUD COMPUTING ENVIRONMENT

The prevailing digital forensics frameworks are not suitable for the cloud environment. A lot of evidence exists in the digital world which needs to be customized and a lot more needs to be handled inbuilt in the Frameworks [23]. The forensic Framework for Cloud Computing Environment lack appropriate standardization. Some of the major challenges observed are scheduled in the Table 2. Specified below. The Table 2 also specifies the Solutions provided by various researchers. A lot of issues are discussed by many researchers [18][20][21][22]. Few challenges are discussed in this section.

(a). Issues regarding Volatile : The important Logs of Virtual machines which hold the significant evidences such as Internet files (URLs accessed), the registry entries logs, and process logs are lost as soon as the Virtual machine instances are closed. If an attack is launched by a malicious user using the Virtual machines instances and then shuts them down. No traces of the attacks are left. To overcome such issues Grispos et al [44] suggested that evidence can be collected when the Virtual instances are powered on or from the RAM of a running computer termed as Live Forensics or Live Investigation. Brik et al [42] provided a solution. Damshenas M et al. [41] proposed the cost globalization amongst CSPs to tender insistent storage device for end user records. Zawoad et al [17] suggested that CSPs can deliver an uninterrupted ceaseless API to clients, and CSPs can assimilate the synchronization method applied to every Virtual Machine and preserve the data / logs in the interiors of their infrastructure. M.K.Waldo et al [11] have advocated to isolate the cloud instance for the forensics investigations. B Hay et al [12] have done the forensic examination of volatile data using a virtual introspection. Virtual machine introspection were also used for Intrusion Detection T Garfinkle [3][26]. This challenge of Volatile data can be categorized under the Identification Stage Step 1 in Figure 2.

(b). Admittance to evidence in Logs: A very significant role is played by the logs in an investigation process. Many researchers have suggested solutions for Admittance to evidence in logs. Such a challenge is categorized under the Identification Stage Step 1 in Figure 2.Many CSPs lack facilities to gather logs and at times intentionally keep such details unknown to Consumers. Gathering of Logs from a cloud domain is a grim process, blended with the complex behavior of clouds and the multi-tenant cloud models, involving a lot many number of diverse users that operate on the similar common processing and network resources. Zawoad et al. [3][8] presented "Secure-logging-as-a-service (SecLaas)" a process defined for Logs on cloud forensics, SecLaas permits CSPs to collect and accumulate logs of the VM's and also aid in access to the investigators . They assure that the confidentiality of the consumers is stays intact. The integrity of the evidences can be verified by via "proof of past log" and the "log chain".

Damshenas et al. [41] recommended a method to design an interface which abstracts significant status of the data in the given system, data pertaining to the consumers only. The author provided read-only accesses to the some specific logs on demand. R Marty et al suggested that every log entry should contain data regarding occurred events like what and why it happened, who initiated the event and when it occurred. The significant fields that are needed to be captured are timestamp, details of the application, consumer, session ID, severity, reason, and categorization. D Birk et al [42] projected a logging mechanism, which is designed to spontaneously signs and encrypts the log information priory and then it's sent to a central logging server which is controlled by the customer. This method will avert budding spies against interpretation and change of log information while storing in Server dedicated for logs.

Trenwith et al [7] designed a model for central logging to track the users' activity during the investigation process. It gathers log evidence and passes all such logs to a remote and central log server. This idea aids and speeds up the evidence gathering during the investigation. This system lacks the security measures required, like access control on the central server. It is the major restriction of the system. Joshia et al. [4] acclaimed the cloud management plane, an interfaces with the cloud infrastructure. The model defined interacts with the file system and the hypervisor on the CSP's Server and is also used to instantiate the VMs and the influence the firewalls [3]. Sang et al [19] proposed a assists in decreasing the difficult issues in forensic activities for actions of non-repudiation. They also suggested that there should be a backup log which is local and synchronous and can be used to keep a check on the activities on the cloud. The CSP does not have to interfere for all this. The log module employs unique identification and the timestamp. Hashing technique was employed to identify any modification if any on the data of log files. As per the researcher Zafarullah et al.[6] logging principles need to be developed. The system developed by them consists of a log management module which gather and correlated the data in the logs. The logs generated need to be preserved as well. They used Eucalyptus setup for the experiments. The Eucalyptus clouds performance was observed and all the different sorts of interactions (internal and external) recorded. Snort was used to log the data. "Syslog and Log Analyzer (e.g. Sawmill)" were also used. These logs were used to analyze the IP addresses of the attacker. The logs recorded employed the different details like how many number of times the http requests were made and at what time, timestamps were employed to give details of the time. The details of the web browser and the fingerprints of the OS of the attacker were also recorded. Patrascu et al. [13][25] [31] presented a framework for logging. The model designed assisted the investigators to analyze the workloads of the VMs. Their methods was also able to handle the scalability issues of a large distributed system. The result observed were very considerable with respect to time.

(c). Issues regarding the Service level agreement (SLA): SLA include all the terms and conditions about the processed of forensic investigations. "If the SLA does not include any notice of what kind of procedure or forensic data should be provided to the consumer, then the CSP has no contractual responsibility to provide such information". The significant terms concerning forensic investigations at times are not a part of the SLA agreed amongst the CSP and the consumer. It could possibly be due to lack of awareness from the consumers, the transparencies lacking from the CSPs, boundaries of trust and issues in the international regulations. CSPs do not give appropriate transparency to the consumers as they themselves lack knowledge on criminal investigations or they are not adapting to standard techniques in their data centers. When a consumer signs a agreement with the CSP concerning the purging of data after the expiry period of the agreement, he has no any technique to verify whether the CSP has actually purged the data or no. If the consumer is violating the SLAs the CSP does not credit the user and such overheads are left to them for providing the evidence for such violations. Such terms may not be acceptable for any enterprise. Most of the SLAs also do not specify the site where the consumer's data would be preserved. These can lead to issues as the server holding the data can be in any country and this country may have many laws and regulations pertaining to that data. SLAs give a better information to the investigating team about the rights of the users and the responsibility of the CSPs. Thorpe et al [30] specifies that the users can be given the right to decide where their data would be preserved specifically in private cloud so as to they are aware of the jurisdictions. Such things need to be specified in the SLA. During the forensic investigations the evidences can be traced on such clouds which are placed in such jurisdictions. A lot of "SLA-based" resolutions are provided try to solve the above issues and also specify the measure for evaluating the performance. K Ruan et al[24] suggested that the SLAs need to include all the significant terms regarding the forensics investigations. Damshenas et [41] stated that the SLAs between the consumer and the CSP have to be very clear and it should Well-written. It should also include policies to preserve the client's policy. Baset et al [45] stated some guidelines concerning the SLAs and its detailed descriptions for cloud services. The guidelines included some significant points regarding the detection of service violation and the credit for the same, the interval of service guarantee and granularity, SLA standards and outcome based SLAs.
Busalim et al[48] recommended a SLA framework for ecommerce cloud. It is a web based system which supports SLA life cycle according to the end user perspective. It states that the SLA should include the significant objectives and parameters. In Bouchenak et al. [68] model for cloud which has priority for Quality of Service (QoS) and SLA. This model can be applied to any cloud. A control-theoretic needs to be followed to be provide the better than the best-effort cloud QoS. Benchmarking tools become a need to obtain better results. The design of services of the cloud should be controllable through construction. Serrano et al [50] developed a "SLA-aware-service cloud model". It describes a nonfunctional interface that revels the related SLA. A QoS oriented SLA for the cloud services has been focused on. It provides online services along with guarantees for cost, performance and also provides dependability. Service level objective like terms were used. They were the means of measuring the performance and it assist in avoiding the disputes occurring between different parties due to misinterpretations. A robust SLA system to effectively fight the cybercrime was suggested by Biggs et al [51]. It suggested that the illegal activities like Distributed Denial of Service ought to be employed to test the cloud vendors system. To assists the forensics procedures a good feedback system needs to be provided .Birk et al[42] recommended the audit service as a measure of security should be provided by the trusted third party. Haeberlen [47] suggested time-stamping system needs to be a logs which cannot be tampered. These are used to detect the SLA violations.

d).Challenge of Encryption categorized under the Examination Analysis Step 3 Figure 2 .Trenwith et al. [7] used AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) algorithms to convert plaintext data to encrypted form. It can be applied to unsecured connections to provide confidentiality and authenticity. AES algorithm is applied to files with large data while RSA algorithm is applied on AES-keys. Wan et al. [52] projected a "Hierarchical attribute-set-based encryption". This encryption was applied to accomplish fine-grained access control in cloud computing. It also achieves scalability and flexibility. Prabha N et al presented an encryption technique for query processing on cloud to safeguard confidentiality[37]

(e). Multi-Tenancy, Integrity and Privacy Issues: Integrity of the evidence is a major concern when applied to all types of cloud services and any system. As stated by many acquiring data legally from multiple jurisdiction is a complex task. One needs to abide by Law as well. Integrity of the logs which server as evidence can be maligned by the CSP or the Hypervisors [8]. Such evidence are not considered valid unless the integrity is proved. According to Aydin M et al[43] stated that the investigators need to be endorsed for the extra added trust needed from the third parties to verify the data to be so called evidence. The elements used in process of integrity verification has to be set beforehand such that it is also acceptable in the court of Law else later it becomes a problematical non trustable source of integrity verification. Martini et al [66] suggested such a challenge is applicable to analysis stage. In cloud environment the users are mapped on the same VMs machines storage. During the repossession of the traces in multi-tenant environment the process must uphold the confidentiality, shield the privacy of the occupants and lastly guarantee that the appropriate data of specific tenant is collected. "Any attempt to physically connect to a data store or virtual host system will have the risk of modifying data that is outside the scope of the investigation as far as belonging to a system that is not possessed or functioned by the suspect named in the warrant" Farina et al[67]. As the environment in multi-tenancy is such that the storage unit is common the users in such environment can contaminate the important traces. Also the privacy of other occupants needs to be well-conserved. The privacy of the users is affected by the issues of multi-jurisdiction and virtual systems. Breaching the users privacy should be avoided the Investigators and they need to assure that all the regulations and the standards are obeyed during the evidence collection process. CSP should support mechanisms such that no team from his organization can have access to user's deleted data.

To certify the integrity of the evidence, Shams et al. [38][68] recommended a digital signature process can be applied to the data collected as evidence and a procedure needs to be defined to check the same later. Hegarty et al. [53] designed a signature detection framework which could be distributed and permits analysis of storage platform from the forensics point. Shi Y et al. [54] suggested a multi-tenancy model for the issues of security on data storage mapped as a successions integrity issues applied on chunks of data.
Yan C et al [55] recommended a new forensic framework for cyber-crime which safeguards the privacy and integrity. It also images the records and files unequivocally. Juels et al. [56] built a "Proofs of retrievability (PORs)" which consists of a back-up service called prover which generates a brief evidence that a verifier (client) has retrieved a file. The POR methods and cryptographic mechanism employed aid in the supporting privacy and integrity of files accessed by the users. Birk et al[42] built a "Trusted Platform Module" which provides assurance on the integrity of a platform. The standard built the researcher traces any changes made to the previous configurations and provides a secure storage as well. Only a single host gets the security in a traditional secured platform but this system designed to provide a

"closed box execution environment" by outspreading the properties of trusted platform to the whole of IaaS system. Damshenas et al[41] stated that the SLA contract should contain the significant points related to the clients privacy. Zhou L et al. [58] projected a "role based encryption (RBE) a pattern which permits the "role based access control policies applicable for the data stored in the encrypted mode on public clouds. The RBE pattern was used like the base to secure the cloud data storage architecture applied to the public and private cloud. Sensitive data of the organization was stored on the private cloud and all other data was stored in the encrypted form on the public cloud. The results observed were possessing efficient performance characteristic. Nancy Ambritta et al [59] recommended a system where a user has to register to get the keys to his data for the specified authority. The system faces some issues in scaling. They developed the Identity and Access Management that which avoids overheads of registration of the users and key management activities. The system manages the privacy. Yang et al. [60] suggested a system to secure the privacy with utmost efficiency. They applied a token based approach for accessing the data on cloud storage. It also supported revocation. The system achieves security in both the forward and reverse way. Trenwith et al. [7] applied Hash algorithms which generates a hash log which is employed like an encryption key to encrypt a salt value and the output of this process the cipher text is saved. It employs the encryption key to encrypt the salt value. Also additions are made to the metadata system. The provenance system proposed by Li Chen et al [61] is equipped with the fine grain access control, tracking the provenance, unforging ability, confidentiality and unspecified authentication.

(f). Lack of suitable forensic tools: A lot of tools currently available are not fitting into the requirements and novel set of tools are required to identify, gather, and analyze forensic data. Biggs S et al stated that Impact of CC will diversely effect digital forensic investigations. The Cloud Forensics Domain lacks the good set of Forensic tools. Josiah et al. [4][5] proposed the tool applicable for forensic process for obtaining data in the cloud from the management plane. It has a web based interface to manage and observe the infrastructure. They resolved the issues and recommended that the system offers the best blend of speed, control and trust. They eit. Internet Evidence Finder and F-Response are employed to collect the different artifacts on various social networks and also from cloud [71]. Juels et al. [56] developed PORs tool which provides privacy and integrity on user files on archives. Its applicable on Semi-trusted archives. Josiah et al. [14] developed a forensic toolkit for Openstack cloud called FROST. It's made up of three new forensics tools. It can be applied to obtain reliable forensic data of Virtual disks, Logs of API and guest firewall.

(g). Time synchronization—reconstruction: the time parameter involved in data of criminal activities is very vital and it requires quite an effort to obtain correct results. The users are spread over the different time zones and use the servers spread over the different zones. User's activities are stored by the servers which also stores the time the activity was performed. Timestamps plays a significant role in the evidence part in the court of Law. The time factor can be easily changed by malicious users, such manipulations promote the investigators to obtain additional evidence which ascertains the activity happening time. An extra effort in needed to reconstruct the crime scene as the facts needs to be placed in the logical order of their occurrences. If the VM instances are forcibly shut down, the volatile data which are potential evidences will be lost and the reconstruction phase is near to impossible then.

To elucidate the time zones' problem, Damshenas et al. [41] advised to apply GMT (Greenwich Mean Time) a time system to all the entities of cloud. This contains the benefit of logical time pattern. In IaaS, the users have a full control on the VMs, so in such cases all the user's data needs to be stored in a specific time pattern. Mills et al [62] suggested the clock synchronization between different terminals to handle the issues in Network Time Protocol. The modern protocol "RFC 5905" is one of the most efficient systems. Kao DY et al [63] suggested a new method to improve the accurateness of date time stamps logs. It's has novel methods to create accessed modified in the support of improving the evidence collection process in the cloud environment. This challenge of Time synchronization—reconstruction can be categorized under the Identification Stage Step 3 in Figure 2.

TABLE 2: MAJOR CLOUD FORENSICS CHALLENGES AND OBSERVED SOLUTIONS

Sr-No	Challenges observed in Cloud Forensics	Solutions Provided	Researcher
1	Issues Regarding Volatile Logs	Live Investigation	Grispos et al[44]
		Data Synchronization	Brik et al [42]
		Cost globalization between CSPs	Damshenas M et al [41]
		API with Continuous Synchronization	Zawoad et al [17]
2	Admittance to evidence in logs	Secure-logging-as-a-service mechanism	Shyams Zawoad et [8]
		Status data extraction and checking	Damshenas M et al [41]
		Log management architecture	R . Marty et al [29]
		Logging mechanism	Birk et al[42]
		Digital forensic readiness model	Trenwith et al [7]
		Management plane	Dykstra J et al[4]
		Log-based model	Sang T et al [19]

		Eucalyptus framework	Zafarullah Z,[6]
		Logging framework	Patrascu et al [31]
3	Issues regarding Service level agreement (SLA)	External auditors	Birk et al[42]
		Well and clear-written terms	Damshenas M et al [41], Ruan K [24], Thorpe et al[30]
		Service guarantee, violation detection, credit and standardization	Baset et al[45]
		Trusted time stamping	Haeberlen et al [47]
		Define SLA parameters and objectives	Busalim et al [48]
		QoS and SLA model	Bouchenak S [49]
		SLA-aware-service	Serrano D et al [50]
		Robust SLAs	Biggs S et al [51]
4	Encryption Issues	Digital forensic readiness model	Trenwith PM et al [7]
		Hierarchical attribute-set-based encryption	Wan Z et al [52]
5	Multi-Tenancy, Integrity and Privacy Issues	SLA contracts	Damshenas M et al [41]
		Digital signature	Zawoad et al [17][68]
		Trusted Platform Module	Birk et al[42]
		Digital forensic readiness model	Trenwith PM et al [7]
		Distributed signature detection framework	Hegarty et [53]
		Multi-tenancy model	Shi Y, Zhang et al [54]
		Cyber-crime forensic framework	Yan C et al [55]
		Proofs of retrievability	Juels A et al [56]
		Trusted cloud computing platform	Santos N et al [57] ,
		Secure role-based access control	Zhou L et al [58]
		Identity and access management in future internet architecture	Nancy Ambritta et al [59]
		Data access control for multi- Data access control for multi authority cloud storage	Yang K et al [60]
		Provenance system	Li J, Chen et al [61]
6	Lack of suitable forensic tools	International legislations and global unity	Biggs S[51]
		Management plane	Dykstra J et al[4]
		Proofs of retrievability	Juels A et al [56]
		Forensic Open-Stack Tools	Dykstra J et al[14]
7	Time synchronization—reconstruction	Unified/specific time system	Damshenas M et al [41]
		Network Time Protocol	Mills et al [62]
		Created-Accessed-Modified model	Kao DY et al[63]

VII. INDIAN CYBER LAWS

Crime in any form and any country unpleasantly touches the entire society. Cyber-crime is any unlawful conduct done by means of electronic set-ups that aims at breaking the security of computer systems and the data processed by them. In developing economies, cyber-crime has augmented at rapid paces, due to the speedy diffusion of the Internet and the digitization of economic activities. The Cyber-Crime threatens the Nation's security and financial health. The Information Technology Act, 2000 deals with the issues like "Legal Recognition of Electronic Documents, Legal Recognition of Digital Signatures, Offenses and Contraventions and Justice Dispensation Systems for cyber-crimes". Cyber-Crime is not demarcated legitimately in IT Act or in any other legislation. But the notion of cyber-crime is a blend of crime and computer. Few of the offences covered under this act are listed in Table 3.

TABLE 3: CYBER CRIMES AND THE PUNISHMENT SPECIFIED AS PER IT ACT 2000/2008

Sr-No	Cyber-Crime Offence	Section-No	Punishment
1	Tampering with Computer Source Documents	Section-65	The criminal would be sentenced to jail for 3 years or levied fine up to 2 Lakhs INR or both
2	Hacking with Computer Systems and Data alteration	Section-66	The criminal would be sentenced to jail for 3 years or levied fine up to 2 Lakhs INR or both. Cognizable, Non Bailable
3	Publishing obscene Information	Section-67	First offence 5 Years imprisonment and adding to it a Fine up to 1 Lakh INR Second and Subsequent offence 10 Years

			imprisonment and adding to it a Fine up to 2 Lakh INR Cognizable, Non Bailable
4	Breach of Confidentiality and Privacy	Section-72	The criminal would be sentenced to jail for 2 years or levied fine up to 2 Lakhs INR or both.
5	Publication of false digital signature certificate	Section-73	The criminal would be sentenced to jail for 2 years or levied fine up to 1 Lakh INR or both.
6	Publication for fraudulent purpose	Section-74	The criminal would be sentenced to jail for 2 years or levied fine up to 2 Lakhs INR or both.
7	Denial of Service Attacks (DoS) Distributed Denial of Service (DDoS) Advanced Persistent Denial of Service Attacks	Section-43 (e),(f) and (g)	The criminal would be sentenced to Imprisonment for 10 Years or so
8	Cyber Terrorism	Section -66F	The criminal would be sentenced to Imprisonment for life

Evidences are very important to prove such Laws. The Integrity of the evidence is all the more vital. If the Evidence or the Integrity of the traces cannot be proved in the Law court, then the convicts cannot be convicted [70].

VIII. Conclusion and Future Work

This paper review focuses on significant areas of Cloud Forensics like Cloud Frameworks, Steps involved in the Cloud Forensic environment, the Challenges and Some few solutions provided by the various Researchers. It becomes vital to comprehend the different categories of the relevant data that may be required to be mined and/or bid in an exploration which involves cloud environment, and hence, additional drill and tools for the forensic investigators to deal with the standard cloud computing data extract formats. The existing digital forensics frameworks are not suitable for the cloud environment. They lack the needed standards. Lawbreakers, malicious users or other such people, are always on the go to find lacunas, to quest novel domains, technologies and prospects in cloud computing environment. They always intend to influence and take advantages of the different weaknesses and openings that would be found in Law enforcement, Commercial sector, Finance Sector, economic or online environments. So there is a necessity to build up the Standardized framework which permit better forensic investigation in cloud and such malicious users can be tracked and punished by Law.

References

[1] Shams Zawoad, Ragib Hasan, and Anthony Skjellum "OCF: An Open Cloud Forensics Model for Reliable Digital Forensics" In the proceedings of 2015 IEEE 8th International Conference on Cloud Computing DOI 10.1109/CLOUD.2015.65 Page No: 437 -444, 2015.

[2] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Muhammad Shiraz, Samee U. Khan, Rajkumar Buyya, and Albert Y. Zomaya. 2016. "Cloud log forensics: Foundations, state of the art, and future directions", ACM Computing Surveys. Volume No 49, Issue No 1, Article 7,42 Pages. DOI: https://dl.acm.org/citation.cfm?doid=2911992.2906149, Page No : 7:1 - 7:42 ,2016.

[3] Stavros Simou1, Christos Kalloniatis, Stefanos Gritzalis and Haralambos Mouratidis "A survey on cloud forensics challenges and solutions" Published in Security and Communication Networks in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1688, Page No: 6285–6314, 2016.

[4] Dykstra J, A Sherman AT. "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques" In the Proceedings of the 12th Annual DFRWS Conference. Digital Investigation. Elsevier, 9 Supplement, 2012.

[5] Dykstra J, A. Sherman, "Understanding issues in cloud forensics: Two hypothetical case studies" Journal of Network Forensics, Vol. b, No. 3, Page No. 19–31, 2011.

[6] Z. Zafarullah, F. Anwar, and Z. Anwar, "Digital forensics for Eucalyptus" in Proceedings of Frontiers of Information Technology (FIT) Page No. 110–116, IEEE-2011.

[7] Trenwith PM, Venter HS. "Digital forensic readiness in the cloud" In Information Security for South Africa. Page No. 1 - 5 IEEE-2013.

[8] Shams Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS: Secure logging-as-aservice for cloud forensics" in Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS) New York, Page No. 219–230, ACM-2013

[9] Corrado Federici, "AlmaNebula: a computer forensics framework for the Cloud" published in the 4th International Conference on Ambient Systems, Networks and Technologies, Elsevier, Procedia Computer Science, 19 , Page Nos : 139 – 146, 2013

[10] Sean Thorpe and I. Ray, "Detecting temporal inconsistency in virtual machine activity timelines", Journal of Information Assurance & Security, Volume. No 7, Issue No. 1, 2012.

[11] M. K. Waldo Delport, Martin S. Olivier, "Isolating a cloud instance for a digital forensic investigation" in Information and Computer Security Architecture (ICSA), 2011.

[12] B. Hay and K. Nance, "Forensics examination of volatile system data using virtual introspection," ACM SIGOPS Operating Systems Review, Vol. No. 42, Issues No. 3, Page No. 74–82, 2008

[13] A. Patrascu and V V. Patriciu, "Logging system for cloud computing forensic environments" Journal of Control Engineering and Applied Informatics, Volume No l0, Issue No. 1, Page No. 80–88, 2014.

[14] J. Dykstra and A. T. Sherman, "Design and implementation of frost: Digital forensic tools for the OpenStack cloud computing platform" Digital Investigation, DOI: https://doi.org/10.1016/j.diin.2013.06.010, Volume. No 10, Page No. S87–S95, 2013.

[15] NIST Cloud Computing Forensic Science Challenges, Draft NISTIR 8006, Page No 1 – 44, June 2014.

[16] Thorpe, S. ,Ray, I. Grandison, T. ; Barbir, A, "Cloud Log Forensics Metadata Analysis", Computer Software and Applications Conference Workshops (COMPSACW), 36th Annual, Date of Conference: 16-20 July 2012, Page No. 194 – 199, E-ISBN : 978-0-7695-4758-9 ,Print ISBN: 978-1-4673-2714-5, INSPEC Accession Number: 13119531 ,conference location : Izmir, Turkey , IEEE-2012

[17] Shams Zawoad, Ragib Hasan "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problem" (arXiv: 1302.6312v1), 26th February-2013

[18] Stavros Simou, Christos Kalloniatis, Evangelia Kavakli, Stefanos Gritzalis "Cloud Forensics: Identifying the Major Issues and Challenges", Springer International Publishing Switzerland 2014. Page No. 217-284

[19] Sang T "A log-based approach to make digital forensics easier on cloud computing" In Proceedings of the Intelligent System Design and Engineering Applications (ISDEA) 3rd International Conference Page No. 91–94, IEEE-2013

[20] H. Guo, B. Jin, and T. Shang, "Forensic investigations in cloud environments" In Proceedings of Computer Science and Information Processing (CSIP), International Conference, Page No. 248–251, IEEE-2012

[21] .S. Wolthusen, "Overcast: Forensic discovery in cloud environments" In proceedings of Fifth International Conference on IT Security Incident Management and IT Forensics (IMF), Page No. 3–9, IEEE,-2009

[22] D. Reilly, C. Wren, and T. Berry, "Cloud computing: Pros and cons for computer forensic investigations," International Journal Multimedia and Image Processing (IJMIP), Volume No 1,Issue No 1, Page No. 26–34, March 2011.

[23] M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, "Digital evidence in cloud computing systems" Computer Law & Security Review, Volume No. 26, Issue No 3, Page No. 304–308, 2010.

[24] Ruan K, Carthy J, Kechadi T, Crosbie M. "Cloud forensics : An overview" In proceedings of Advances in Digital Forensics VII, 7th IFIP WG 11.9 International Conference on Digital Forensics, Volume No 361, Peterson G, Shenoi S (eds), Berlin Heidelberg, Page No. 35–46, Springer-2011

[25] Alecsandru Patrascu, Victor Valeriu Patriciu "Logging for Cloud Computing Forensic Systems" International Journal of Computer Communications and Control, ISSN 1841-9836, 222 Page No: 222 - 229, April, 2015.

[26] T. Garfinkel and M. Rosenblum, "A virtual machine introspection based architecture for intrusion detection," in NDSS, San Diego, CA, February 2003.

[27] A. Srivastava and J. Giffin, "Tamper-resistant, application-aware blocking of malicious network connections," in RAID, Boston, MA, September 2008.

[28] B. D. Payne, M. Carbone, and W. Lee, "Secure and flexible monitoring of virtual machines," in ACSAC, Miami, FL, December 2007

[29] R. Marty "Cloud application logging for forensics" In Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, New York, NY, Page No. 178–184. 2011

[30] S. Thorpe, T. Grandison, A. Campbell, J. Williams, K. Burrell, and I. Ray "Towards a forensic-based service oriented architecture framework for auditing of cloud logs" ,In Proceeding of the IEEE 9th World Congress on Services, Page No 75–83. 2013a

[31] A. Patrascu and V. V. Patriciu.. "Logging framework for cloud computing forensic environments" In Proceeding of the IEEE 10th International Conference on Communications (COMM). Page No 1–4. 2014.

[32] K. L. K. Ryan, P. Jagadpramana, and B. S. Lee "Flogger: A file-centric logger for monitoring file access and transfers within cloud computing environments", In Proceedings of the International Joint Conference of IEEE TrustCom-11/11/IEEE ICESS-11/FCST-11, Page No. 765–771 2011a..

[33] Sean. Thorpe, I. Ray, and T. Grandison "Enforcing data quality rules for a synchronized VM log audit environment using transformation mapping techniques", In Computational Intelligence in Security for Information Systems. Springer, Berlin, Page No 265–271, 2011c.

[34] Sean. Thorpe, I. Ray, I. Ray, and T. Grandison. 2011d. "A formal temporal log data model for the global synchronized virtual machine environment", In the Journal of Information Assurance and Security, ISSN 1554-1010,Volume No 6, Issue No 2 , Page No 398–406, 2011.

[35] Sean. Thorpe, I. Ray, I. Ray, T. Grandison, A. Barbir, and R. France "Formal parameterization of log synchronization events within a distributed forensic compute cloud database environment". In Digital Forensics and Cyber Crime, Springer, Berlin, Page No 156–171, Springer-2012b

[36] M. Sato and T. Yamauchi. "Secure log transfer by replacing a library in a virtual machine". In Advances in Information and Computer Security. Springer, Berlin, Page No 1–18. 2013.

[37] N. Prabha, C. Timotta, T. Rajan, and A. Jaleef PK. "Encrypted query processing based log management in the cloud for improved potential for confidentiality". International Journal of Computer Applications in Technology. Res. 3, 5, Page No 309–311, 2014 .

[38] Shams Zawoad, Marjan. Mernik, and Ragib. Hasan "Towards building a forensics aware language for secure logging", Computer Science and Information Systems, 11, 4 , DOI: 10.2298/CSIS131201051Z, Page No 1291–1314,2014.

[39] Chen G. Du Y, Qin P, Du J. Suggestions to digital forensics in cloud computing ERA. In Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on. IEEE, 2012; 540–544.

[40] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems" IEEE Cloud Computing, Volume. No 3, Issues No. 1,Page No. 50–59,IEEE- 2016

[41] Damshenas M, Dehghantanha A, Mahmoud R, Shamsuddin bin S. "Forensics investigation challenges in cloud computing environments" In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012\ International Conference. 2012; Page No 190–194 ,IEEE-2012.

[42] Birk D, Wegener C. Technical issues of forensic investigations in cloud computing environments" In Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop , Page No. 1–10, IEEE-2011.

[43] Aydin M, Jacob J. "A comparison of major issues for the development of forensics in cloud computing." In Information Science and Technology (ICIST), 2013 8th International Conference for. Page No. 77–82, IEEE-2013.

[44] Grispos G, Storer T, Glisson WB. "Calm before the storm: the challenges of cloud computing in digital forensics" International Journal of Digital Crime and Forensics (IJDCF), IGI Global: Hershey; 4(2) Page No. 28–48,2012.

[45] Baset SA. Cloud SLAs: present and future. ACM SIGOPS Operating Systems Review. ACM 2012; 46(2), Page No. 57–66.

[46] Mishra AK, Matta P, Pilli ES, Joshi RC. "Cloud forensics: state-of-the-art and research challenges". In Cloud and Services Computing (ISCOS), 2012 International Symposium ,Page No.164–170 IEEE-2012.

[47] Haeberlen A. "A case for the accountable cloud". ACM SIGOPS Operating Systems Review. 44(2) Page No 52–57 ACM -2010.

[48] Busalim AH, Hussin ARC, Ibrahim A. "Service level agreement framework for e-commerce cloud end-user perspective". In Research and Innovation in Information Systems (ICRIIS), 2013 International Conference Page No. 576–581, IEEE,-2013;

[49] Bouchenak S, Chockler G, Chockler H, Gheorghe G, Santos N, Shraer A. Verifying cloud services: present and future. ACM SIGOPS Operating Systems Review, 47(2):Page No 6–19 . ACM -2013.

[50] Serrano D, Bouchenak S, Kouki Y, et al. "Towards QoS-oriented SLA guarantees for online cloud services" In Cluster, Cloud and Grid Computing (CCGrid), 2013 \13th IEEE/ACM International Symposium ,Page No 50–57 IEEE- 2013;

[51] Biggs S, Vidalis S. Cloud computing: the impact on digital forensic investigations. In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference Page No 1–6, IEEE-2009.
[52] Wan Z, Liu JE, Deng RH. HASBE: "A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. Information Forensics and Security, IEEE Transactions 7(2),Page No 743–754 , IEEE- 2012;.
[53] Hegarty R, Merabti M, Shi Q, Askwith B. "Forensic analysis of distributed data in a service oriented computing platform". In Proceedings of the Convergence of Telecommunications, Networking & Broadcasting, PG Net, 10th Annual Postgraduate Symposium on Liverpool. 2009.
[54] Shi Y, Zhang K, Li Q. A new data integrity verification mechanism for SaaS, In: FL Wang, Z Gong, X Luo, J Lei (eds). Web Information Systems and Mining. WISM 2010 International Conference. Springer: Berlin Heidelberg, Page No. 236–243 ,2010.
[55] Yan C. Cybercrime forensic system in cloud computing. In Image Analysis and Signal Processing (IASP), 2011 International Conference Page No.612–615, IEEE, 2011
[56] Juels A, Kaliski Jr BS. "PORs: proofs of retrievability for large files", In Proceedings of the Computer and communications security, 14th ACM conference on. ACM: Alexandria, VA, USA, 2007; Page No. 584-597
[57] Santos N, Gummadi KP, Rodrigues R. "Towards trusted cloud computing", in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing (HotCloud'09). 2009.
[58] Zhou L, Varadharajan V, Hitchens M. Achieving secure role-based access control on encrypted data in cloud storage. Information Forensics and Security IEEE Transactions , Page No. 947–1960, IEEE 2013.
[59] Nancy Ambritta P, Railkar PN, Mahalle PN. Proposed identity and access management in future internet (IAMFI): a behavioral modeling approach. Journal of ICT Standardization. River Publishers 2(1), Page No 1–36 , 2014.
[60] Yang K, Jia X, Ren K, Zhang B, Xie R. Effective data access control for multiauthority cloud storage systems. Information Forensics and Security, IEEE Transactions 8(11) Page No. 1790–1801, IEEE -2013.
[61] Li J, Chen X, Huang Q, Wong DS. Digital provenance: enabling secure data forensics in cloud computing. Future Generation Computer Systems 37:259–266 ,2014.
[62] Mills D, Martin J, Burbank J, Kasch W. Network time protocol version 4: Protocol and algorithms specification. IETF RFC5905,2010.
[63] Kao DY. "Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments", The Journal of Supercomputing Page No. 1–20, 2015.
[64] Ben Martini, Kim-Kwang Raymond Choo "An integrated conceptual digital forensic framework for cloud computing " Page No 71 – 80 Digital Investigation Elsevier -2012
[65] https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf [Accessed online in December 2016]
[66] Martini B, Choo KKR. "An integrated conceptual digital forensic framework for cloud computing". Digital Investigation 2012; Volume No 9, Issue No 2, Page No 71–80,2012.
[67] Farina J, Scanlon M, Le-Khac NA, Kechadi M. "Overview of the forensic investigation of cloud services". In Availability, Reliability and Security (ARES), 10th International Conference 556–565 , IEEE, 2015
[68] Shams Zawoad, Ragib Hasan, Anthony Skjellum " Towards achieving reliable digital forensics in IaaS and Stass Clouds using the open cloud forensics model" in Services Transactions of Cloud Computing (ISSN 2326-7550) Volume N. 4, Issue No. 3, July-September 2016
[69] https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/ [Accessed on 31-March-2018]
[70] http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf [Accessed on 31-March-2018]
[71] Chen L, Xu L, Yuan X, Shashidhar N. Digital forensics in social networks and the cloud: process, approaches, methods, tools, and challenges. In Computing, Networking and Communications (ICNC), International Conference on. IEEE, 2015; 1132–1136
[72] Mustafa Aydin and Jeremy Jacob, "A comparison of major issues for the development of forensics in cloud computing", 8th International Conference for Internet Technology and Secured Transactions (ICITST- 2013).