IJoFCS (2012) 2, 64-74

e-forensic PRESS

The International Journal of FORENSIC COMPUTER SCIENCE

www.IJoFCS.org

DOI: 10.5769/J201202005 or http://dx.doi.org/10.5769/J201202005

Forensic Investigation in Cloud Computing Environment

Agreeka Saxena, Gulshan Shrivastava, Kavita Sharma
Department of Information Technology,
Dronacharya College of Engineering, Gr. Noida, U.P., India
agreeka07@gmail.com, gulshanstv@gmail.com, kavitasharma_06@yahoo.co.in

Abstract - Cloud Computing has been in its boom stage since a long time. Although the exact definition of Cloud Computing have a cloudy appearance in the Information Technology environment -in this paper, the related definition of cloud computing along with computer forensic has been explain. Various computer forensic measures and merits are explained. Also the concerns of users before using cloud computing have been judge.

Key-words - Cloud Computing, Cloud Forensic, Forensic approach, a new approach - an Endeavour, Digital Evidences.

1. Introduction

The correct definition of cloud computing still has a cloudy appearance in I.T. world. But in a layman concern "Cloud computing is the collection of some information, which resolves users query per its requirement".

Perhaps the definition of cloud computing can be the process of accessing the data and related information as per end user requirement along with the services provided by the vendor chosen by end-user. The data related information could be anything like files or programs, etc.

"Cloud" the term can be used as data hub where all the require data of user gets store and is delivered to the user whenever been asked by him. In today's era the computing world is heading towards the cloud computing technology and environment, with the matter of fact of its advancement. The advancement driven up by cloud computing environment is first:

i. 99.99% availability stream [2]
ii. Strong network infrastructure
iii. Platform independency to run applications.
iv. Powerful connectivity if internet
v. Gigantic data hub

Cloud computing can even be defined as the further more extension of cluster computing that is cloud computing is inheritance of cluster computing along with it services.

Paper submitted on October 4th, 2012.

2. Services

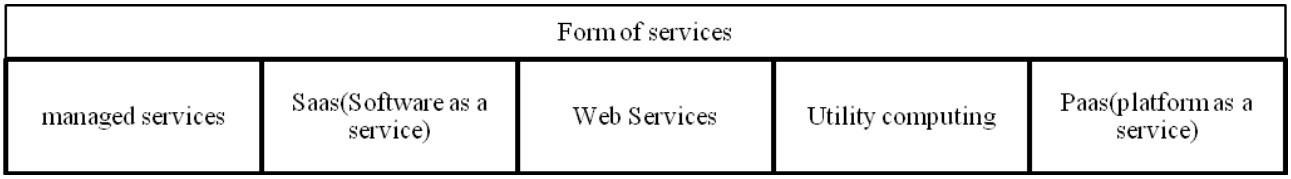

Fig. 1 (Services of cloud computing)

2.1 Managed Services:

It manages the services or application delivering criteria. In fact it believes in handing over the application directly to enterprise rather than delivering it to end users. Such enterprises act as mediators, which finally provides with the users with the services in forms of application. E.g.: Gmail provides spam filtering service, CenterBeam provides desktop management [1] etc.

2.2 Saas*:*

Software as a service are the application service providers, i.e., they are the vendors which provide customers with the application services. For instance purpose they run a single major application is data hub and provide the rest functionality to end users though to end users through internet server. The various Saas vendor are Ramco, SAP, Oracle (for ERP applications), oracle (CRM application) and so on.

Various search engines as well as social networking sites such as facebook, orkut, twiter, etc, are among the Saas agent's providers.

2.3 Web Service:

Another form of Saas can be termed as web services. The only difference is Saas providers and web services is that, web services providers APIs is the various numerous application developers, that can be helpful and display in no. of applications [1] for instance: smart card processing system etc.

2.4 Utility Computing:

Cloud computing defines its concept of computing through its utility service, which can term or determined as the basic us ability of services. It basically offers the vital computing resources such as virtual server & storage services [1] for instance: There are various providers or companies that provide their end users with virtual windows desktop for those who cannot afford them in real for instance:- Desktop two , Sun Micro system etc [1].

2.5 Paas:

Platform as services is the further extension of Saas, i.e., it emerges out from Saas only. It in totality provides a plot form (environment) for the application developed and it authentically involves computing resources for initializing the application [1], for instance:- Python - based application was developed by using Google app engine also initialized the application with no cast up until 500mb of storage.

3. Characteristics along with Delivery and Deployment Models:

The totality of Cloud Computing can be understood and be explained by characteristics and delivery models along with the essential deployment models [2].

3.1 Characteristics of Cloud Computing:

i. Multiple network access simultaneously.
ii. Prominent Flexibility.
iii. Pay as per resources demanded.
iv. Independent resource ditching.
v. Services as per demand.
vi. Cloud independency.

3.2 Delivery Models:

Saas (Software as a service) : application service provider to end users.

Paas (Platform as service) : providing platform for deployment of application service.

Iaas (Infrastructure as a service) : providing infrastructure resources like storage, network bandwidth, etc.

3.3 Deployment Model:

Before the deployment model, the characteristics are needed to be fulfilled along with the delivery models, which play a vital role in deployment of a "cloud".

i. Internal cloud: - Especially design for private enterprise and owned by them with safety measures.

ii. External Clouds: - Such clouds are open to all i.e. they are publicly available mega infrastructure.

iii. Multiple clouds: - They are the composition of more than one cloud to form any element cloud.

iv. Troop Cloud: - Troop Sharing of infrastructure for similar functionality of various troops.

4. Architecture Proposed

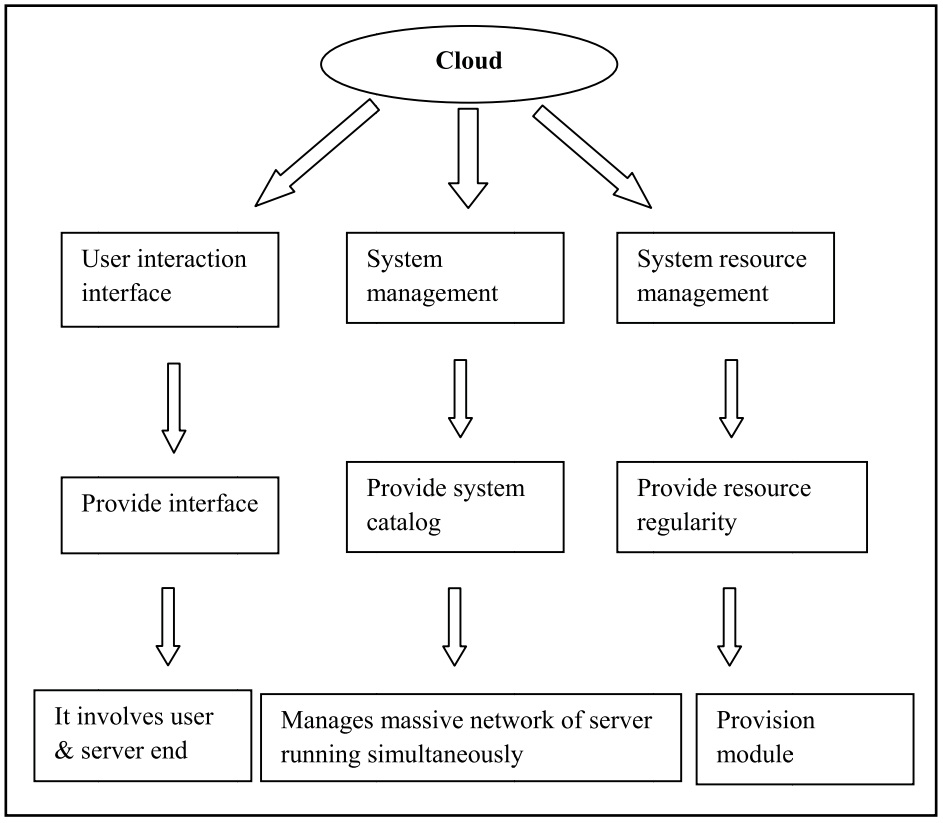

Figure 2 (Proposed Architecture1 of Cloud Computing)

The proposed architecture defines Cloud Computing as: User Interface, System management, System Resource management. Where further User Interface imparts interface between user and server end. Precisely it involves user end as well as server end. Along with System management provides system catalog. Also it manages the massive network of server that are running simultaneously as per required by user. The System Resource Management imparts resource regularity i. e. the regularity of resources has been confirmed by System resource management. Also it provides Provision modules for regularity.

5. Existing Architecture:

The already existing Architecture defines the three different further architectures: Physical, Geographical and Logical.

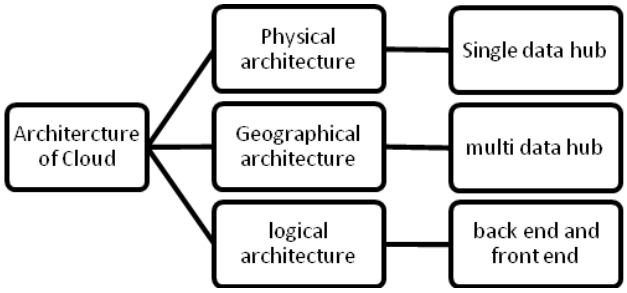

Fig.3 (Existing architecture of Cloud Computing)

5.1 Physical architecture:

Clients demand for resources are flexible amongst themselves due to which the physical servers are not been able to run with fulfillment to overcome such problem the technique of virtualization is adopted, in such a technique more than single operating system multiple virtual OS runs on a single system which decrease the demand for peripheral device.

Firstly, from Data hub centre nodes are being computed as per the service category. Again those nodes are connected in a suitable topology, that are further been connected to the network. Then finally, these services are delivered to front end i. e. to the organization. Physical resource set are the end users.

5.2 Geographical Architecture:

It comprises for similar structure that of physical structure, the only difference is that, in geographical architecture there are number of services.

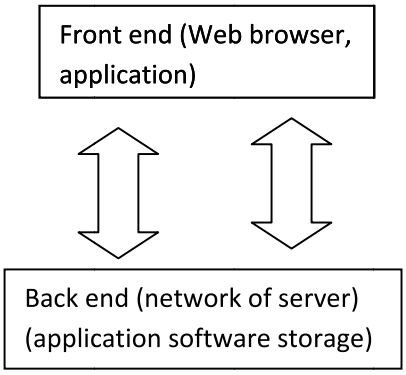

Fig. 4(Logical architecture)

5.3 Logical Architecture:

Back end of the logical architecture follows a three tier systematic view.

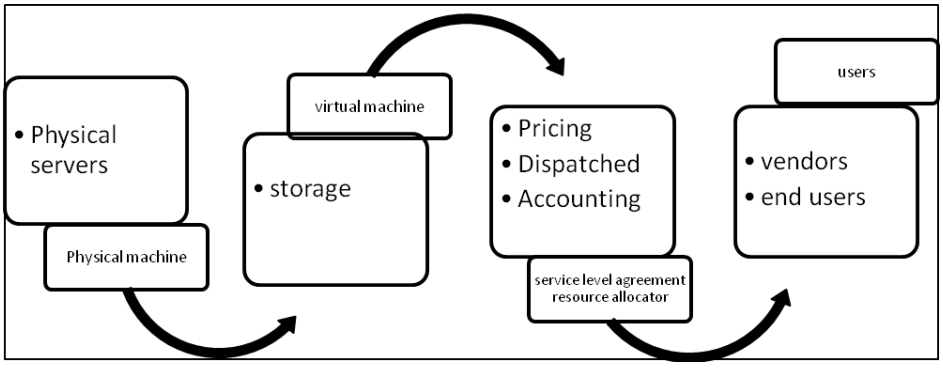

Fig. 5 (Logical architecture) [2]

The Service Level agreement comprises of the contract for the monitoring of services that satisfies the user requirements. SLA even includes the jurisdiction I.e. justice along with data possession. This specifies that, particular application and its data and a service belongs to a particular client with whom SLA is formed. It even includes output of utilizing the services by some other end user.

6. Computer Forensic

It involves the investigation done at computer level for the evidence of any crime that has occurred by some computer Digital medium. More authentically, it is termed as "Digital Forensic" to classify the applied process in forensic performed by some digital devices that run over some operating system.

Digital Forensic involves:

i. Computer Forensic: The fundamental factor of computer forensic is to retrieve data along with guideline and procedure to create legal audit. This audit needs to be presentable in court and to be effectively acceptable.

ii. Intrusion Forensic: The functionality intrusion forensic is refers to detect the intrusion attack or any suspicious attack of any sort of malicious user. It even involves any doubt-able attack against the system.

iii. Network Forensic: The fundamental work of intrusion forensic is to refer any natural source evidence towards crime & criminals through which the crime can be investigated further. It involves keeping track of network accessing factor. In further content; network along with intrusion forensic will tackle the issue of network forensic.

iv. Mobile Forensic: It refers to the crime that is being conducted through mobile phones as their medium. As the users of mobile phones are maximum in today's era therefore, maximum crime are being conducted through it only.

In whole, the forensic involving cloud computing technique considerably involves computer forensic along with some advances of intrusion network forensic. The actual definition of cloud forensic is cloudy as like cloud computing but alternatively, "computer forensic can termed as information that can act as a proof to determine crime characteristics efficiently evidence through digital medium". Digital medium can even be replaced by computer medium.

7. Cloud Forensic

Cloud Forensic can be defined as a subpart of Network Forensic also it is a core application within Digital Forensic [7]. Which means Cloud Forensic is a part of both- Network forensic as well as Digital Forensic.

It is also a cross over product of Cloud Computing and digital Forensic. That means it investigates about the attacks taking place through digital medium in the cloud world. Secondly, it is a sub category of Network Forensic because all crimes investigated are carried over Network Layer. As a result of which all the crimes are usually detected at Network Layer only. It follows the set of techniques and measures to catch away the crime in cloud environment.

7.1 Detection of Crime in Cloud Environment:

To detect any crime which is being held or about to be held in the cloud can be done by following certain measures. These measures could be followed at fundamental levels as well as high level too. That may involve various safety measures that need to be implemented by cloud service providers. Few of such measures are

i. Malicious User Detection:

The measures can be taken to detect whether the user who have login to the account is genuine or some malicious user, who wants to retrieve the data of some other real users.

a. To attain this measure cloud service provider can ask the user to generate more complex and strong password at the time of creating his account.

b. The service provider can use a multi-way security verification code check every time when user login to his account.

c. The cloud system could be set in such a way that every time when the user login to his account, a verification question can be asked by system whose answer should match with the real data saved in the cloud database.

ii. Secured Protocol:

The protocol involves in the cloud environment should be made more secure and advance, which can assure more security to user's data.

UDP is an unreliable protocol which should be avoided in the data packet transfer, whereas on the other hand **https** is a secured protocol which should be taken in consideration by cloud service. Such protocols impart security to the user data at the time of data transfer from one user account to the other.

iii. Session Security:

In order to impart safer cloud environment to the user, the session created should be of lesser period of time which means sessions should be made secured by reducing the time interval of session expiry.

With this process, it would be difficult for hacker to peep into the session of some user.

8. A New Approach- An Endeavour

Digital Forensic as defined by NIST is the application of science to identification, collection, examination and analysis of data while preserving the integrity of information and maintaining a strict chain of custody for data [8].

Therefore it is an attempt for investigating the crime. It is an approach to get through the root cause of the crime which ultimately leads to the criminal mind behind it. The various approaches of forensic in cloud environment are

8.1 Snapshots: Snapshots are a mean by which a client can preserve any specific state of virtual machine. This paper reviews that not only the client but also the service provider can keep a track of what clients are doing in the cloud and can have snapshots of any suspicious act.

The virtual cloud states can easily lose their integrity as they are accessible by both client and the service provider. But also a service provider can keep an eye over the acts of client and can keep a record, if the act is suspicious in his view, some way or the other. And once the snapshot from service provider end is being taken it can be freeze and its integrity can be maintained.

8.2 Network layer: The OSI model provides information about each layer individually as well as it imparts information or integration of the layer. Network layer in the system do not provide log data from its respective components. Also of the malware infection occur at Iaas Virtual Machine, it would be difficult to retrieve any routing information.[8]. To overcome such problem various security checks can be applied at network layer. Also, the security check have to quality to store the data and information which has been passed through it. That could a precise way to investigate about crime at cloud level.

8.3 System Layer of Client: The services of cloud are communicated directly with client system layer. In fact, it is the only application that interacts with the services imparted by cloud. The system layer at clients end or the client system layer totally dependent on the delivery models of cloud computing only if the correct evidence of crime needs to be extracted. Hence, the delivery models need to be governed by service providers and no alteration should be allowed or accepted from client end.

8.4 In-volatile Data: Although virtual Iaas model do not hold persistent storage of the information. For instance AWS EC2 cloud instance, all volatile data get lost if that instance is shut down or if it is rebooted. To overcome

such situation where, sensitive data can be deleted by the user. The Cloud Service Provider makes use of in volatile technique for all sort of sensitive, fragile data. The cloud environment should provide verification process that does not allow the client to verify the fragile data stored on Virtual Machine and cannot delete it exhaustively.

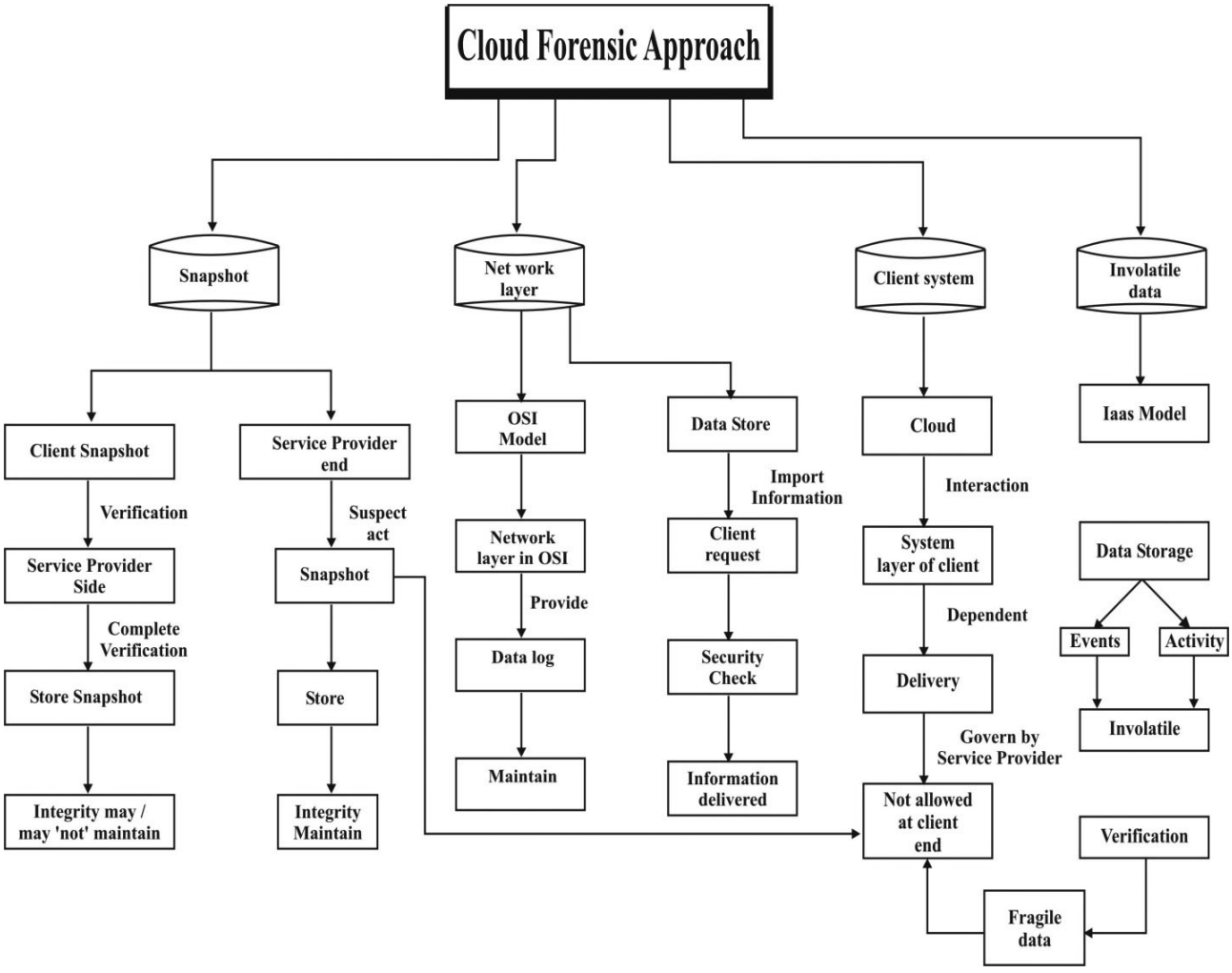

Fig. 6 (Cloud Forensic approach)

9. Digital Evidence

Digital evidence can be defined, “information or data of vital use that has develop through some digital medium”.

The digital evidence may involve files store, memory data, virtual memory data in form videos or snap shots etc transferred over some network [2].

9.1 Characteristics of digital evidence:

i. Quality evidence: whatever is the data that has been gathered through digital medium, but it is acceptable if and only if, it hold some quality standard according to requirement of court.

ii. Crime depicter: the evidence should be clearly describing the crime conducted; there should not be any rest of manipulation in evidence.

iii. Vast no. of suspects: the server in the network has been used by multiple users due to which there are several suspects.

iv. Original products: rebooting process may manipulate the evidence & disturb the authentication of the data.

Digital evidence must fulfill the characteristics mention above along with which it should also follow the legal requirement that are necessary:-

i. Complete: the evidence should not lack features that put a question over completion of evidence also; it should be complete enough to guilt the criminal.

ii. Authenticated: the evidence used should be original without any sort of amendment made from investigator`s end.

iii. Integrity: whatever data or evidence provided by investigator should consist of necessary information to that the governing body can rely on it without any doubt.

iv. Admissible-the evidence collected must have followed the legal & legislative procedure.

v. True: whatever is the data or evidence gathered it should be enough to convince the authorities.

9.2 Issue with Digital evidences:

i. The only drawback with digital evidence is that it involves both logical and physical construction. [2]

ii. The data in which is an evidence is stored in some physical content (media storage) [2]

iii. The physical content must is forms of blocks [2]

iv. The overall data or content is gathering together at logical content.

v. Due to which at the time of investigation both physical as well as logical construct need to be go through simultaneously.

9.3 Need for Dynamic Evidence:

The evidence gathered, if been static evidence, are alone not acceptable by the authority as a full proof evidence. With a matter of fact evidence required are the collection of related facts that are collectively on whole alter the digital environment in which the crime happened. Computer forensic is actually not termed as science but is termed as interest of creation or art in simpler words. Computer forensic focuses on altering the whole event with the evidence which is available to the investigator. Though the process is time consuming in real time because it requires first, working individually on every event, then integrating these events and again working on this respective integration, which was actually a time acquiring process.

To overcome this issue the concept of time lining was evolved [2].

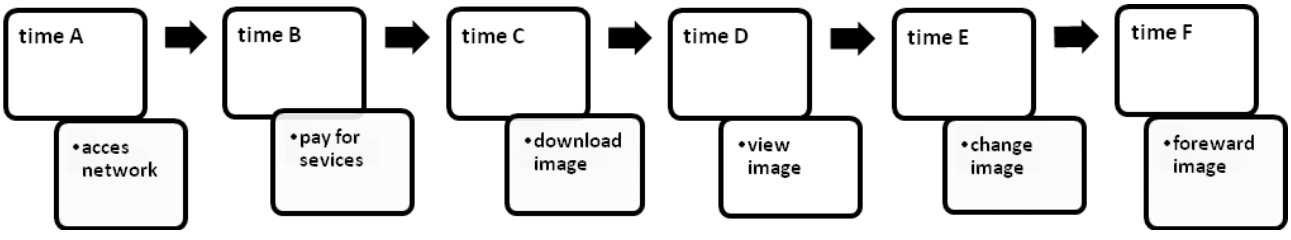

Fig. 7, [2] (time line technique)

10. SIX stages Model for procedure:

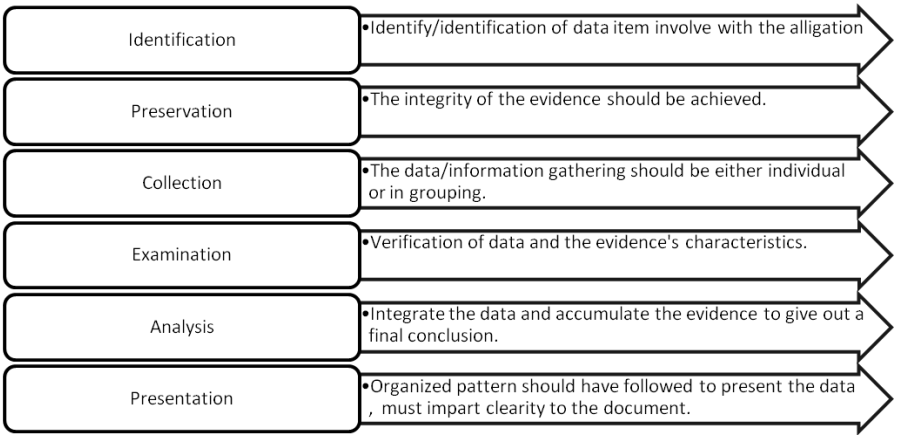

Fig. 8, [2](Six stage model for forensic evidence)

Procedure:

Along with digital evidence, computer forensic investigation also involves the procedure with respect to the model process. The procedure or model process involves the fundamental steps need to follow to obtain a complete investigation. This involves the theoretical as well as practical feature of an investigation procedure.

The Association of Chief Police Officer (ACPO) guidelines for computer investigations & electronic evidence [2] is a complete documentation which reveals the accurate procedure that should be followed with the evidence when associated with computer & digital evidence.

The guidelines also follow certain principles to prove that the evidences are reliable and can be accepted in court for further procedure. The procedure is followed to maintain the integrity of the document. It is useful for the investigation of the case accordingly.

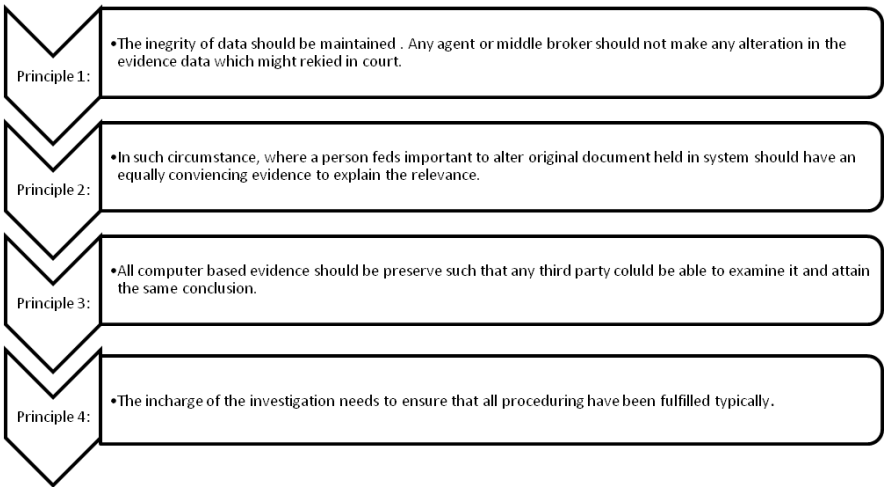

Fig. 9[2] (Principle of legal evidences)

11. Involvement of Cloud in Forensic

The uses of abundant computing resource are in era due to which the maximal crime incidents occur with the hi-tech approach and due to which the crime rate is increasing rapidly in the world. In the country about 82 percent own their

Mobile phones while 73% population in UK has their own mobile phones [3]. The estimation reveals that 6 out of crime commits are mobile phones which include almost every sort of crime, roads accident, murder etc.

Cloud computing is the major step of development and it is actually a huge where almost all the IT companies are falling in. however, where it comes to forensic cloud computing is a matter of doubt for implementation. Though cloud computing has in valued the issue of security & the major of security in an important issue to its environment as it hold numerous data & information of end-users the security is the major aspect to think ever. Due to security issue only cloud computing is forensic has got a setback. Individual to organizations one can afford to have an insecure environment to work with is. They do not want any unauthorized access to their data in any situation. Due to which cloud computing investigation need to go through its development phase again to get implemented is computer forensic & sustain its value in it.

Virtualization for computer forensic:-

Virtualization is a technique where there single operating system is installed on a physical system virtually. The main advantage of virtualization is that with is cloud many resources can be virtual: server, storage capacity software platform network infrastructure etc.

This concept is implemented through VM where & citrixxenserver [2].

Virtual machines provide a user with several advantages for instance VM ware provide snapshot facility[2], which provide the picture of system after interval at the time of snapshot. This provides computer for the picture of an image in the system hard disk that comprises of information of hard disc, VM ware configuration and BIOS configuration [2]. There are various snapshot files that collected in the content but even on whole the VM source is questionable. That is because there are changes in VM ambiance when VM image is booted into new ambiance that alters the original data.

12. Merits of cloud computing

i. Centralized data availability, data available in all places provide the forensic spontaneity and readiness

ii. With infrastructures, a service vendor can construct and authenticated forensic server in the cloud.

iii. The services n platform provided by cloud computing makes a mark able importance in forensic.

iv. Availability of high storage capacity and maximum availability of 99.99% provides a great spontaneity to forensic investigators

v. The job work could be made easier with the intense resource in the cloud

vi. Additional inbuilt hash functions authentication of disc images

vii. Concept of virtualization, to decrease the cost of various recourses such as storage, software etc

viii. Accessibility from anywhere

ix. Manipulation of resources per uses requirement.

Adoption concerns:

Before adopting the concept & technology of cloud computing there are various concerns about which a user always think off. Such issues are more in end users than in an enterprise. Concerns are:

1. Accessibility:

Providing a 100% availability is almost an impossible scenario until, we adopt an extremely availability platform technical architecture. For example in the end of January Wikipedia was unavailable for whole one day for the Intellectual property issue, blackberry services were unavailable for 24 hours in august 2011.

In such situations:

a. Enterprise should maintain a backup data.

b. Uses should keep desktop version so that they can work offline even when the cloud server is down.

c. Major concern is, when the providers exhale the market or when they face problems in delivering the services.

2. Security & integrity:

Due to malicious user illegal act makes the data vulnerable to various attacks with a response to which a provider should provide the latest update technical protection measures to the users. Enterprises pay for the support services provided by providers, individual users are left on their own.

Vendors should provide support service to them too. In fact they should provide more user friendly cloud computing environment to such users.

3. Inter-operability:

It is a technique, by which the application of various service providers can be combined & can be deployed. This technique use to lack in 2008 but now the concept has been taken into consideration.

13. Conclusion

Cloud Computing is a technology that involves the file assessment and processing of the files as per the requirement of the client. Forensic is a technique in which the evidences collected are verified. In whole when clouds computing and forensic are interlinked that leads to Computer forensic. This technology collects the crime evidences that have been conducted through computers. This paper involves the definition of cloud computing along with forensic & its vivid types involved I computer forensic. Concept of cloud computing is lacking somewhere in its security aspect due to which it is yet not prominently accepted in forensic branch. But its future scope might be efficiently effective in forensic era.

REFERENCES

[1] "Cloud Computing: "Status and Prognosis", in Journal of Object Technology, vol. 8, no. 1, January-February 2009, pp. 65-72 http://www.jot.fm/issues/issue 2009 01/column4/.

[2] Cloud Computing: pros and cons for Computer Forensic Investigations.

[3] Stephenson, P., Modeling of post incident root causes analysis, International Journal of Digital Evidence, Volume 2, No. 2, 2003.

[4] http://cloudcomputing.blogspot.com/Cloud computing: adoption fears and strategic innovation opportunities.

[5] J. Nicholas hoober and Richard Martin: "Demystifying the Cloud", InformationWeek Research & Reports, Pp.30-37, June 23, 2008.

[6] J. Nicholas Hoober: "Outages Force Cloud Computing Users To Rethink Tactics", InformationWeek, August 16, 2008.

[7] Chen, Y.J.Wang, L.C., "A Security Framework of Group Location-Based Mobile Applications in Cloud Computing",International Conference on Parallel Processing Workshops, Pp.184-190, 2011.

[8] R. Howard, R. Thomas, J. Burstein, and R. Bradescu, "Cyber Fraud Trends and Mitigation", in The International Conference on Forensic Computer Science (ICoFCS), 2007. Available: http://dx.doi.org/10.5769/C2007001

[9] J. H. M. Nogueira, "Ontology for Complex Mission Scenarios in Forensic Computing", in The International Conference on Forensic Computer Science (ICoFCS), 2007. Available: http://dx.doi.org/10.5769/C2007006

[10] G. M. Nunes, "Instant Messaging Forensics", in The International Conference on Forensic Computer Science (ICoFCS), 2008. Available: http://dx.doi.org/10.5769/C2008002