RESEARCH ARTICLE OPEN ACCESS

Challenges and Proposed Solutions for Cloud Forensic

Puraj Desai, Mehul Solanki, Akshay Gadhwal, Aalap Shah, Bhumika Patel
Department Of Computer Science and Technology Uka Tarsadia University Bardoli, Surat, Gujarat 394350
Department Of Computer Science and Technology Uka Tarsadia University Bardoli, Surat, Gujarat 394350
Department Of Computer Science and Technology Uka Tarsadia University Bardoli, Surat, Gujarat 394350
Department Of Computer Science and Technology Uka Tarsadia University Bardoli, Surat, Gujarat 394350
Assistant Professor Department Of Computer Science and Technology Uka Tarsadia University Bardoli , Surat, Gujarat 394350

Abstract
Cloud computing is a heavily evolving topic in information technology (IT). Rather than creating, deploying and managing a physical IT infrastructure to host their software applications, organizations are increasingly deploying their infrastructure into remote, virtualized environments, often hosted and managed by third parties. Due to this large scale, in case an attack over the network of cloud, it's a great challenge to investigate to cloud. There is a very low research done to develop the theory and practice of cloud forensic. The investigator has huge challenge of getting the IP address of the culprit as there is dynamic IP in cloud computing. Also one among many problems is that the customer is only concerned of security and threat of unknown. The cloud service provider never lets customer see what is behind "virtual curtain" which leads customer more doubting for the security and threat issue. In cloud forensics, the lack of physical access leads to big challenge for investigator. In this paper we are presenting few common challenges which arise in cloud forensic and proposed solution to it. We will also discuss the in brief about cloud computing and cloud forensic.
Keywords-Cloud Computing, Virtual Environment, Cloud Forensic

I. INTRODUCTION

Cloud forensic is a popular and less expensive as well as efficient way of storing data today. Many firms and organizations have joined with the cloud services to keep their application or other data available 24*7 online.

With the increasing use there always stays risk of data security and privacy. Here is where cloud forensic is needed but still cloud forensic is not much developed theory. According to the author in [1], there are many complicated problems faced by investigator during collection of data also there are different types of issue on which investigator has to come across to get the evidence of suspect.

The investigator has various problem like the storage of data is not local once kept on cloud thus suspects computer cannot have anything stored in the computer, then comes second problem that the data stored on cloud is of multiple user so the server cannot be seized else all the users data are seized.

Third problem is data of suspect is found but still separating it from other users data is complex. Once the data is on cloud the theft can be done so it's a high risk for health related data, national data, security related data. There are different challenges like data acquisition, logging, chain of custody, limited forensic tools, trustworthy data retention, etc

Digital storage of computer data is carried out more these days as cloud computing provides great infrastructure for organizations and individuals. Due to large scale use of storage there can be attack over the network and hence it would be a big challenge to investigate on cloud. For investigating purpose the digital forensic is newly used with increasing use of digital storage over virtual network and also for the criminal activity.

According to the author in [2], the main problem while investigating on network is from where (Location) the attack has been carried out, due to IP address not static over cloud computing its complex task to retrieve the IP address. Also there are different types of challenges like government aspects, risk factor and control suffered by forensics. Even there are few issue like threat and security issue, data security and privacy issue, trust issue suffered by them.

In [3], the author has proposed that the use of cloud computing increasing the security concerned challenges is also increasing. Digital provenance is an important feature of digital forensic which leads to use different tools and techniques. Also the source retrieved is to be proved by digital forensic, thus it's mandatory to have exactly data and digital forensic need to separate data from other user on the cloud. Also there can be attack over cloud like DDos and unauthorized file sharing carried out on the cloud.

Computing over cloud is a heavily promoted and enhanced way to store data, as its resource dependent there is research being carried out for different types of opportunity and also to analyse and do experiment

over it. Cloud computing consist of different concepts like network computing, utility computing, software as a service, storage on cloud and virtualization which is been done by IT technicians for unification in information processing.

Cloud refers to provide services to client remotely. According to the author in [4], many businesses are moved to cloud due to long time availability of data and also to use few or more needed application remotely. There are few security issues like regulatory compliance, data location, privileged user access, data segregation, recovery, and investigative support. There is a challenge for live forensic tools to grab the IP address and to get evidence too over virtual environment like cloud.

In [5], the author has proposed that cloud computing is most discussed topic but still it presents many economic opportunities and promising technology. There is an open issue of performing digital investigation over cloud. As there is lack of physical access to server, it's a mere challenge for investigation. Access is not provided due to effect on customer and provider of insecurity. The nature of data processing on cloud is decentralized and also the evidence collection and recovery approach are traditional which leads to no practical data.

Information technology is a setup of infrastructure for an organization with few boxes of hardware, applications, network switches, data canters, etc. According to the author in [6], the visualization of few computers connected with server and network for sharing different types of things like application, data with a low cast, maintenance free IT infrastructure which is called "Cloud".

Cloud is an environment of elastic elimination of resources which involves multiple stakeholders and provides a measured service at multiple impurities for a specified level of service. Cloud Technology is replacing traditional setup with virtualized, remote, on-demand software services, configured for the particular needs of the organization.

These services can be hosted and managed by in-house or by a third-party. Resulting, the software and data including business application may be physically stored across many different geographic locations. The use of cloud computing has potential benefits to organizations, including increased flexibility and efficiency. On the other side, along with flexibility, efficiency and substantial cost saving, Cloud is also gives a thread to the organization about a theft of Copy Right or patented methods, solutions, or personal or organizational confidential information.

In case of any Cyber Incident, normally, digital forensic investigator assumes that the storage media under investigation is completely within the control of the investigator. Conducting investigations in a cloud computing environment presents new challenges, since evidence is likely to be ephemeral and stored on media beyond the immediate control of an investigator [6].

II. BACKGROUND

In this section, we provide a short overview of cloud computing and computer forensics.

A. Cloud computing

Definition—According to the definition by the National Institute of Standards and Technology (NIST), "Cloud computing is a model which provides a convenient way of ondemand network access to a shared pool of configurable computing that can be saved easily and released with small management effort" [7].

Classification according to service model:

According to the nature of service model used by the Cloud Service Provider (CSP), cloud computing can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [7].

Software as a Service (SaaS). This model provides the users the facility of using cloud service provider's software running on cloud infrastructure. Unlike other software to be installed by the user in machine the user can directly use the same software with the help of cloud which leads to easiness of accessing proprietary software too. Some Examples of SaaS are: Salesforce [11], Google Drive [12], and Google calendar [13].

Platform as a Service (PaaS). In PaaS, user can deploy their own application or a SaaS application in the cloud infrastructure. Normally, the user pay according to the bandwidth usage and database usage. User can only use the application development environments, which are supported by the PaaS providers. Two examples of PaaS are: Google App Engine (GAE) [14] and Windows Azure [15]. User can host their own developed web based application on these platforms.

Infrastructure as a Service (IaaS). This model allows a user to rent processing power and storage to launch own virtual machine. One of the important features is that the user can scale up according to their requirement. It allows their applications to handle high load smoothly. On the other hand, they can save cost when the demand is low. Customers have full control over storage, deployed applications, OS (Operating System), and possibly limited control of selecting networking components (e.g., host firewalls). An example of IaaS is Amazon EC2 [16]. EC2 provides users with access to virtual machines (VM) running on its servers. User can install any operating system and can run any application in that VM. It also gives the customers the facility of saving

the VM status by creating an image of the instance. The VM can be restored later by using that image.

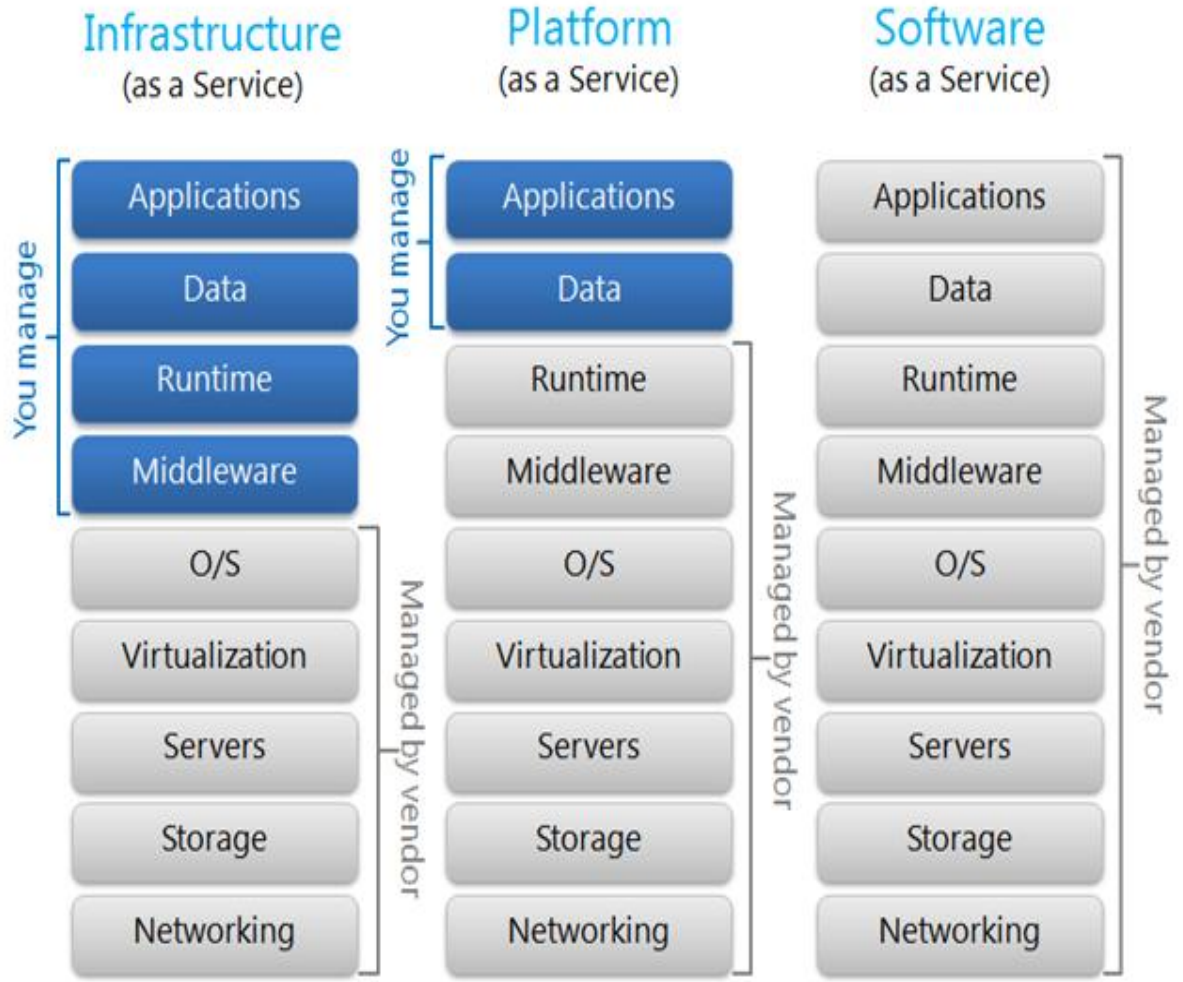

Figure 1: Three service models of Cloud Computing [20]

Classification according to deployment model:

Cloud computing can be categorized into four Deployment model categories – private, public, community, and hybrid [7].

Private cloud.

In private cloud model, the cloud infrastructure is fully operated by the owner organization. It is the internal data centre of a business organization. Private cloud can be found in large companies and for research purpose.

Community cloud.

If several organizations with common concerns (e.g., mission, security requirements, policy, Textile market and compliance considerations) share cloud infrastructure then this model is referred as community cloud.

Public cloud.

In the public cloud model, the Cloud Service Providers (CSP) owns the cloud infrastructure and they make it available to the general people or a large industry group. All the examples given in the service based cloud categorization are public cloud.

Hybrid cloud.

The hybrid cloud infrastructure is a combination of two or more clouds. Hybrid Cloud architecture requires on-premises resources and remote server based cloud infrastructure. Figure 2 shows three different deployment models of cloud computing – private, public, and hybrid cloud.

Figure 2: Three different cloud deployment models [21]

B. Cloud Forensic

Cloud forensic is a domain that works towards the usage and execution of digital forensic policy and methodologies within the cloud.usage of digital forensic in corporate communication amongst the cloud actor to comply with internal and external investigation.

From the definitions, we can say that computer forensics is comprised of four main processes:

• **Identification**: Identification process is comprised of two main steps: identification of an incident and identification of the evidence, which will be required to prove the incident.

• **Collection**: In the collection process, an investigator extracts the digital evidence from different types of media e.g., hard disk, cell phone, e-mail, and many more. Additionally, he needs to preserve the integrity of the evidence.

• **Organization:** There are two main steps in organization process: examination and analysis of the digital evidence. In the examination phase, an investigator extracts and inspects the data and their characteristics. In the analysis phase, he interprets and correlates the available data to come to a conclusion, which can prove or disprove civil, administrative, or criminal allegations.

• **Presentation:** In this process, an investigator makes an organized report to state his findings about the case. This report should be appropriate enough to present to the jury.

Figure 3 illustrates the flow of aforementioned processes in computer forensics.

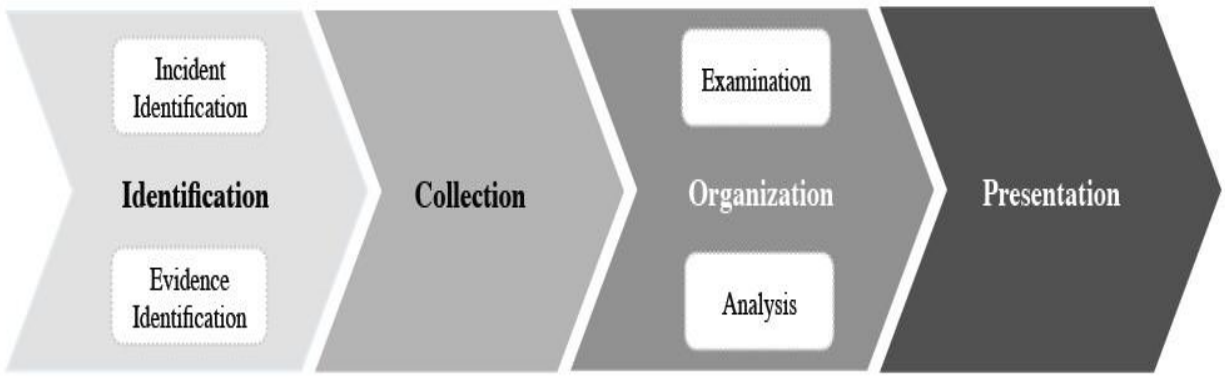

Figure 3: Flow of Computer Forensic [1]

III. CHALLENGES OF CLOUD FORENSICS

In this section, we examine the challenges in cloud forensics, as discussed in the current research literature. We present our analysis by looking into the challenges faced by investigators in each of the stages of computer forensics (as described in Section II-B). Some of the important challenges we address here are: forensic data gathering, limitation of forensic tools, trust issue.

A. Forensic Data Gathering

Collection of the digital evidence is the most crucial step of forensic procedure. Any errors that have occurred in the collection phase will contact to the evidence organization and reporting phase, which will eventually affect the whole investigation process. According to Birk, evidence can be available in three different states in cloud–at rest, in motion, and in execution [5].

Physical Inaccessibility.

Physical inaccessibility of digital evidence makes the evidence collection procedure harder in cloud forensics. The established digital forensic procedures and tools assume that we have physical access to the computers. However, in cloud forensics, the situation is different. Sometimes, we do not even

know where the data is located as it is distributed among many hosts in multiple data centres. A number of researchers address this issue in their work [5].

Mapping IP (Internet protocol) address for Search Warrant.

To issue a search warrant the search warrant should specify the location.in the digital environment the location can be tracked with the help of IP (Internet Protocol) address which is a tedious task in the cloud environment as the IP (Internet Protocol) address is not static.

Volatile Data.

With extra payment user can get storage which is uncommon for small, medium scale business hub. A dangerous user can exploit this blame. A malicious user may complain of the instance being exposed to some third personal and being attacked by him such a scenario is a turmoil for forensic investigation. Without capability of persistence, state would only exist in Random Access Memory, and would be lost when this Random Access Memory loses power as in shutdown of computer [5] [9] [10] [17].

B. Limitations of Current of Forensic Tools.

The flexible feature of cloud paradigm poses as a hurdle for current forensic tools and methodology. The limitations of current forensic tools are discussed by some researchers in their work [17], [18], [6]. For investigations in virtualized environment still there is a lack of tools and procedure. Ruan et al. explained the need of forensic tools and forensic data collection within cloud service provider [18].

C. Trust Issue.

Once the search warrant is issued, an employee of cloud service provider is required for data collection but data collected by employee cannot be validated as the employee cannot be said as a licensed forensics investigator and it is also not possible to claim that data are appropriate. The date and time stamp can also be given after manipulation if it comes from multiple systems. [19]

IV. Tools for Cloud Forensic

Analysis:

- From the analysis we came to know about different problems like
  - API is not available from Cloud Service Provider- The service provider doesn't provide any type of API to investigator to investigate over server which leads to complexity.
  - Security and privacy related issue- Each server consist of multi user and the investigator cannot seize over the server just to investigate as there can be data which are private and also related to national security.
  - IP capturing- the investigator need to have a search warrant before investigation and it is mandatory to specify the IP address(location) as in the digital environment the location can only be tracked with the help of IP address and capturing a Dynamic IP address is again a tedious task.

Experiment:

- There are different types of tools used by digital forensic to retrieve evidence, recover data, etc. One among the data recovering is Autopsy.

- **Autopsy**
  - Autopsy is a memory recovering open source tool which is being used by digital forensic while recovery of data is to be made. This tool helps to retrieve audio, video, image, folders, etc.
  - The tool provides the description of data to be retrieved with the data it was deleted. It also retrieves the data which are permanently deleted from the hard Disk. Once the recovery is done the tool lets the data to be stored on machine back.
  - We tried retrieving an image file which we deleted a week before and we were even successful in getting it.

- **F-response**
  - It is easy to use, vendor neutral, patented software utility which helps to investigate.
  - Data Recovery, Discovery over IP network using tools can be carried out in this tool.
  - Autopsy is totally subset of f-response. Thus, all the features of autopsy can be used in this tool also.

V. Proposed Solution

We assume that the following 3 steps are already being done:

Step 1- To wait for request from the cloud service provider.

Step 2- To gather requirement about the attack.

Step3- Co-operation of the cloud service provider to investigate over the server.

Now, the following steps can be done once the above steps are fulfilled:

Step1- We use the F-response tool as it helps to investigate, it would recover the data, and Discovery over IP network.

Step2- If f-response is not successful in recovering of the data the Autopsy tool can be used.

VI. CONCLUSION

- We identify that cloud forensics is a cross-discipline between digital forensics and cloud

computing. Various aspects of forensic in cloud computing and the cloud forensic have been reviewed. With more use of cloud computing, there is an issue for providing trustworthy cloud forensic schemes. According to current scenario of the world, more business organizations are moving data on cloud environments. As there is development in IT sector, there will be more complexities for crime investigator in accessing, retrieving and getting the data as evidence. With more technology the crime can be done easily (Cybercrime) and demand of forensic investigation on cloud will be more. These investigations have to suffer from lack of guidance, tools and technique to retrieve evidence in forensically good way. Also cloud service provider should provide robust API for acquiring evidence. Solving all the challenges of cloud forensics will clear the way for making a forensics-enabled cloud and allow more consumers to take the advantages of cloud computing. There is also the need for re-examine laws because of the need to move forward and combating criminals. Finally, there is also the need for the digital forensics community to begin establishing standard empirical mechanisms to evaluate frameworks, procedures and software tools for use in a cloud environment. Only when research has been conducted to show the true impact of the cloud on digital forensics, can we be sure how to alter and develop alternative frameworks and guidelines as well as tools to combat cyber-crime in the cloud.

REFERENCES

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

[2] Farid et al. "*A Survey about Impacts of Cloud Computing on Digital Forensics* ", 2013(ISSN: 23050012).

[3] Deoyani Shirkhedkar and Sulabha patil, "*Design of digital forensic technique for cloud computing* ", june-2014(ISSN: 23217782).

[4] Ashish et al. "*Some Forensic & Security Issues of Cloud Computing*", October-2013(ISSN: 2277128x).

[5] Dominik Birk," *Technical Challenges of Forensic Investigations in Cloud Computing Environments*," in Workshop on Cryptography and Security in Clouds, January 12, 2011.

[6] G.Grispos et al. "*Calm before the storm: The challenges of cloud computing in digital forensics*," International Journal of Digital Crime and Forensics (IJDCF), 2012.

[7] P. Mell and T. Grance, "*Draft NIST working definition of cloud computing-v15,*" 21. Aug 2009, 2009.

[8] K. Kent et al. "*Guide to integrating forensic techniques into incident response*," NIST Special Publication, pp. 800–86, 2006.

[9] H. Guo et al. "*Forensic investigations in cloud environments*," in Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, 2012, pp. 248–251.

[10] S.Wolthusen, "*Overcast: Forensic discovery in cloud environments,"* in proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics (IMF). IEEE, 2009, pp. 3–9.

[11] Salesforce, "*Social enterprise and crm in the cloud - salesforce.com*," http://www.salesforce.com/, 2014, [Accessed October 5th, 2014].

[12] Google, "*Google drive*," https://drive.google.com/start#home, [Accessed October 5th, 2014].

[13] ——, "*Google calendar*," https://www.google.com/calendar/, [Accessed October 5th, 2014].

[14] GAE, "*Google app engine*," http://appengine.google.com, [Accessed October 5th, 2014].

[15] Azure, "*Windows azure*," http://www.windowsazure.com, [Accessed October 5th, 2014].

[16] Amazon EC2, "*Amazon elastic compute cloud (amazon ec2),"* http://aws.amazon.com/ec2/, [Accessed October 5th, 2014].

[17] D. Reilly et al. "*Cloud computing: Pros and cons for computer forensic investigations*," International Journal Multimedia and Image Processing (IJMIP), vol. 1, no. 1, pp. 26–34, March 2011.

[18] K. Ruan et al. "*Cloud forensics: An overview*," in proceedings of the 7th IFIP International Conference on Digital Forensics, 2011.

[19] J. Dykstra and A. Sherman, "*Understanding Issues in Cloud Forensics: Two hypothetical case studies,"* Journal of Network Forensics, vol. b, no. 3, pp. 19–31, 2011.

[20] Service Model of Cloud, https://www.spkaa.com/plm-in-the-cloud-computer-system-validation-in-fda-regulated-industries, [Accessed October 5th, 2014]

[21] Cloud Deployment Model,"*vmware.com*", http://download3.vmware.com/vcat/documentation-center/index.html#page/Service%2520Definitions/2%2520Service%2520Definitions.2.03.html,[Accessed October 5th, 2014]