REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

An Analysis Of Improved Forensics Design Framework For Cloud Computing In Computer Reliability System Engineering

Chaudhary Ashish[1*], Milind[2]

[1*,2]Department of Computer Science and Engineering, SCRIET Chaudhary Charan Singh University Meerut
ashishchaudhary3015@gmail.com , milindccsu@yahoo.com

Abstract
The popularity of An Analysis of Improved Forensics design Framework for Cloud Computing in Computer Reliability System Engineering has been growing over the past decade due to the fact that cloud resources can be distributed as needed and are shared by numerous users. According to a recent poll, cybercriminals have been successful in by means of cloud computing skill for fraudulent tasks because of its fundamental features and the dearth of digital forensic methods that are appropriate for the cloud environment. Investigators who handle cloud forensics encounter a number of difficulties and problems while trying to prevent cloud crime. The difficulties that forensic investigators encounter have discussed in this essay. The majority of study work focuses on figuring out the problems with cloud forensics, and the solutions that have been recommended and published in the literature rely on the use of Cloud Service Providers (CSP) for forensic inquiry. Data gathering for the forensics process is one aspect of the reliance on the Cloud Service Provider (CSP), and there's a potential that data manipulation could have an impact on the entire scientific process. To reduce the reliance on CSP, a innovative technique aimed at obtaining forensic indication external of the cloud atmosphere is industrialized.

Keywords: Cloud Computing, Cloud Forensics, Digital forensics, Cloud Forensics Model, Cloud Forensics Trials, Forensic Explanations, Forensic Tool Kit, Cloud Service Provider.

1. Introduction

1.1. Cloud Forensics

"Cloud computing forensic science" refers to the application of technology techniques, developed and tested procedures, and scientific principles to reconstruct historical cloud computing occurrences. To do this, digital evidence is acknowledged, collected, stored, looked at, interpreted, and reported. As shown in Fig. 1, Ruan et al. precise cloud forensics as "The Utilization of Digital Forensic Science in Cloud Surroundings as an A portion of Net Forensics".
Here, the writers emphasize the implication of cloud forensics from three angles: legal, organizational, and technical. Forensic techniques, gear, and procedures involve technical features. The relationship between cloud actors is incorporated into administrative features for forensic investigation. Situations involving many tenants and jurisdictions are covered by legal elements. The authors additionally classify cloud forensics as a subset of digital forensics and cloud computing.

Related Work

Enterprise versions of these technologies have never been tested or authorized but they do include remote forensic proficiencies.
A Digital Data capture tool Standard that frameworks the necessities for digital broadcasting capture tools used in computer forensic investigations is also available from the (NIST, 2004).
The greatest current form of the standard was created in 2004, which predates cloud computing as we recognize it today. More than a few academics have noted that gathering evidence is a significant challenge for cloud forensics. Dykstra and Sherman's examination of two fictitious situation revisions exemplified the non-trivial challenges in retrieving sign from a cloud offence.
The "crystal clear distinct isolation of functions between client and provider" should regulate how volatile and non-volatile cloud data are obtained, according to (Ruan et al., 2011). However, they did not explain who should collect the data or how. Mourned the deficiency of suitable tools for cloud data as well, pointing out that "many of these programmers' have been optimized for current's computing atmosphere, such as EnCase or the Forensics Tool Kit."
Virtual machine introspection allows an external observer to interact with an operating system client through the use of a hypervisor. In 2003, Garfinkel and Rosenblum presented the first demonstration of an interference exposure technique inside a virtual guest using VMI. In 2009, Symantec demonstrated how to use VMware's VMSafe to introduce anti-virus software onto a virtual machine hosted by the hypervisor.
EnCase and FTK have been highlighted as the most popular products with the most worldwide assistance. But these technologies are not without flaws. In 2007, for example, a weakness in the validation between the server and the remote EnCase agent was discovered. From a legal standpoint, court choices or statute law pertaining to the intricate authorized issues nearby remote data achievement are not included in Guidance Software's personal "EnCase Permissible Journal" for 2011, which is a thorough analysis of lawful problems and conclusions regarding electronic discovery. We are examining how cloud computing forensics and lawful search and seizure statutes overlap. For remote forensics, EnCase

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Enterprise and FTK provide with a client-server functionality. A tiny executable (referred to as a "servlet" by EnCase and a “agent" by FTK) is installed on the client computer in each scenario.

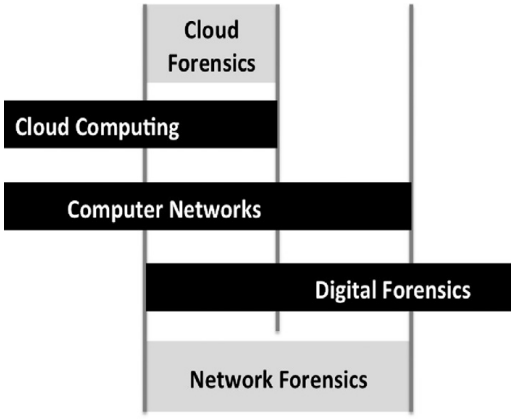

Fig. 1 Forensics in the Cloud

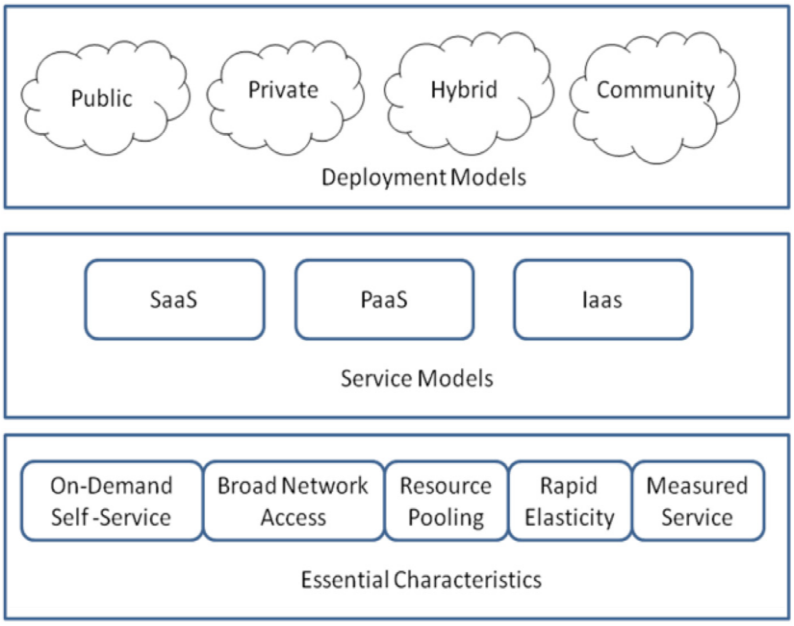

Fig.1.2 NIST Cloud Model

1.2. Cloud Computing

Forensics in the Cloud the inspired Text The sharing of computer resources by several users is known as cloud computing. A public pool of flexible computing properties (such as nets, servers, loading, apps, and facilities) that can be rapidly released and deployed without further effort from management teams or service providers is what the cloud computing architecture seeks to provide. As stated in Fig. 2, the cloud model currently consists of each of the following five primary elements: four deployment models (communal, isolated, mixture, and community), lightning-fast flexibility, on-demand self-service, wide net admittance, measured service, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and lightning-fast elasticity.

1.3. Digital Forensics

"An applied science to recognize an occurrence, assortment, check, and study of mark info" is what digital forensics is defined as. Digital forensics is divided into the following phases:

•*Identification***:** This phase consists of two main steps: identifying malicious action and isolating evidence that points to malicious behavior.

•*Assortment*: Evidence of malicious conduct is gathered from many digital media platforms, and the evidence's integrity is preserved.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

•*Association*: This phase comprises the examiner looking at the evidence that has been compiled for the examination, and all evidence that has been found is correlated with the malicious behaviors.
•Presentation: Based on his investigation into the case, the investigator provides the jury with a properly organized report.

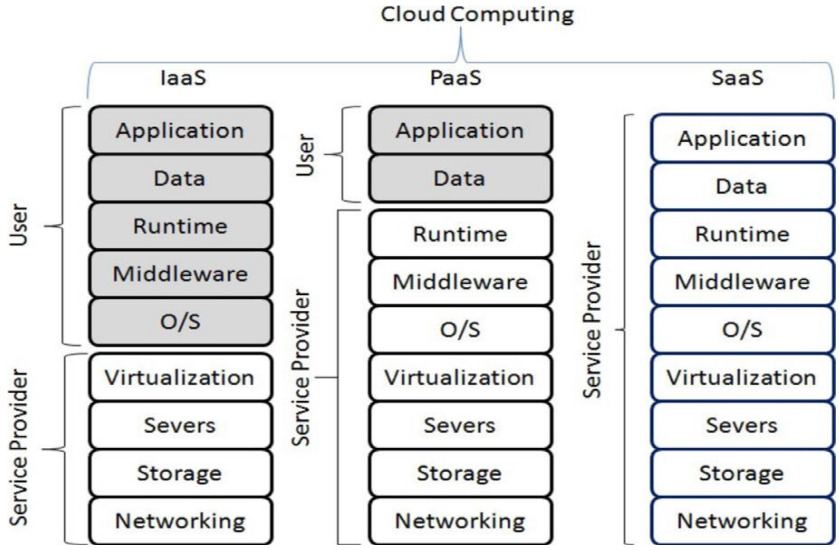

Fig.1.3 Access Management for The Service Architectures

2.Methods

We measured the test's success for each trial using an independent control system that wasn't cloud-based. A Dell computer operating 32-bit Windows 2008 R2, with a single 30-GB disc drive and 2 GB of RAM, served as the control mechanism. After installing the Apache web server, we linked the computer to the Internet. Some internet sides with distinctive tags and content were made by us. A few files were removed. We used a web-based vulnerability to deliberate compromise the machine, and we anticipated that forensic and criminal investigations had started. We used FTK and EnCase to picture the drive.

Experiment 1 examined the purported capacity of well-known technologies to gather forensic evidence at the guest OS (Layer 5) in the cloud autonomously. The capability of the device to gather suggestion remotely and the reliability of the data in evaluation to individuals from an independent regulator mechanism would be the two main indicators of success or failure. We set up a single 64-bit Windows 7 Enterprise forensic examiner workstation that was linked to the Internet via a proxy. The SAFE (Secure Certification for EnCase) component of EnCase Enterprise 6.11 was installed in accordance with the creator's directives. FTK 3.2 was additionally set up. We set up a fresh virtual machine in Amazon EC2 to mimic the subject of a probe. This computer had a Windows 2008 R2 32-bit picture from Amazon that included a single 30 GB hard drive and 1.7. The Amazon firewall is set up to individual certification Remote Desktop Protocol (RDP) (tcp/3389).

We established an RDP connection with the target computer, just as we did with the control system, and then we carried out typical user actions to configure a web server. After downloading and installing Apache, we made a number of web pages with distinctive titles and contents. A few files were removed. We used a web-based vulnerability to artificially compromise the machine once more, and we presumed that a criminal and forensic inquiry had begun.

The remote user programmers that interface with their host server organizers is EnCase Servlets and FTK Agents. There are several ways to use each. Representatives are usually installed to Windows workstations via a net consuming Windows file shares in a corporate setting. The products similarly support physical file transfer via USB, for example. We executed the agent after transferring it over RDP to the target virtual computer in our experiment. We changed our firewall to enable connectivity with the agent: our user-defined port, tcp/3399, was used by the FTK agent, and the EnCase servlet, on tcp/4445.

Version 2.9.0 of FTK Picture Lite was also tested. The product was run interactively after being copied from the examiner's desktop over the Remote Desktop connection. FTK Picture Lite is self-sufficient after it is uncompressed and doesn't require installation. In order to do this testing, we connected a second 100 GB storage capacity and stored a picture of the first disc that FTK Picture had taken. Lastly, we created three 1.7 GB snapshots of the system memory by running Fast dump, Memorize, and FTK Picture.

By inserting an agent inside the virtual computer (Layer 4), Experiment 2 evaluated widely used forensic techniques at the virtualization layer. Once more, the tool's ability to gather indication and the accurateness of the data in comparison to a stand-alone control machine determined the tool's success or failure.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Using a Dell computer running the Ubuntu operating system, the Eucalyptus cloud platform (Eucalyptus, 2011). For managing virtual machines, Eucalyptus supports the Xen hypervisor. A library called LibVMI (LibVMI, 2011) is used to monitor guest operating systems under Xen. We wrote to the visitor computer-generated machine's memory using the LibVMI package. We used this functionality to show how to immediately inject an FTK Agent and an EnCase Servlet into a guest that was already executing. Similar to Experiment 1, we spoke with representative over the net.
Experiment 3 used Amazon's Export capability (Layer 3) to evaluate forensic collection at the host operational structure level. The technique that is most likely employed to comply with subpoenas and search warrants is most similar to this experiment because the information is transferred from a datacenter on Amazon's internal network.
While the storage device is in its possession, AWS also keeps track of its chain of custody. Our criteria for success or failure were (a) the method's capacity to gather evidence and (b) the data's correctness in comparison to the results obtained from the independent switch machine. AWS Export entails sending a storage device to Amazon and submitting a service request. Regretfully, data may only be exported from an S3 container at this time not from an EBS. loudness.
In order to comply with that requirement, we connected the hacked computer's EBS volume to a Linux virtual machine (VM) and utilized to store a picture of the size in an S3 container. We sent a Seagate Free Agent eSATA external hard drive and asked AWS to distribute this container. A copying of the data was given back with the storage device.

Table 1-Six steps of the IaaS cloud atmosphere and probable forensic acquisition procedures for individually, together with the cumulative belief essential through respectively layer

Layer	Cloud layer	Achievement method	Trust mandatory
6	Visitor application/data	Hang on data	Visitant operating system (OS), hypervisor, congregation OS, h/w, net
5	Guest OS	Remote forensic software	Guest OS, hypervisor, host OS h/w, net
4	Containerization	Contemplation	Hypervisor, host OS, h/w, network
3	Host OS	Admittance virtual disk	Host OS, hardware, net
2	Physical h/w	Admittance physical disk	h/w, net
1	Net	Packet capture	Net

3.Result
We were clever to remotely obtain a hard drive and memory picture in Experiment 1 after the EnCase Server and FTK mediator had been installed effectively manually. An accurate chronology of events, including the setting up of Apache and the net web pages we produced and removed, was obtained through examining the pictures in EnCase Forensic and FTK Researcher, correspondingly. No oddities or anomalies that might cast doubt on the data's integrity were found during the study of the virtual environment. Our ability to usage the distant mediators in addition the system bandwidth to transport the data constrained the acquisition process's speed. Afterwards, it took EnCase and FTK about 12 hours each to transfer the 60 GB disc picture and 4GB memory picture using our university's OC-12 connection.
A complete picture of the drive and an accurate time frame were produced by Experiment 2. A potent forensics tool, virtual machine introspection enables live host inquiry while concealing the investigator's identity. But introspection is a distinctive feature that the company providing the cloud services needs to put in place. We were only able to cryptographically confirm the picture's integrity in this experiment because we could equivalence the hash principles of the EnCase picture with the unique disc because we had physical disc access.
Case picture and the innovative floppy. The AWS transfer progression in Experiment 3 also magnificently refunded a whole picture of the floppy. We were clever to load this floppy hooked through nope hitches, in addition confirmed the insides of the drive. An extra profit of this way is that AWS produces a log statement with meta data for individually file distributed. This description confined the succeeding for separately file: timestamp of the allocation, position scheduled the storage device, MD5 check sum, and figure of bytes. These data are protected in a S3 container that we definite in the distribute demand. Our data arrived after five days with expedited shipment, which cost $125. This technique seems to be very similar to what AWS does in order to obey with a subpoena or search authorization.
FTK and EnCase were the easiest to use. The tools' features were widely recognized and easy to use, even though using the remote capabilities needed some setup and learning time. Our disc picture was retrieved in 12 hours, which is much less time than the 5 days needed for the AWS Export procedure for this data amount. 2.5 GB of data are potentially taken on average every hour. Our data was loaded by AWS Export in 4 hours, while the outstanding 116 hours were disbursed in transportation. When additional than 240 GB of data is regained, the export procedure is the most time-effective option at up-to-date rates. The results of the data collection in EC2 are compiled in Table 2. Every tool and method produced proof in an effective manner, but they all impose a high degree of self-assurance in the cloud set-up across the board.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Table 2-Outcomes of three tests receiving cloud-based forensic sign by means of current tools, together with the period to recover the data and faith mandatory in the caller (OS), hypervisor (HV), host (OS), host h/W, net, and Amazon Web Services (AWS) gears.

Testing	**Tool**	**Proof collected**	**Clock (hrs.)**	**Trust required**
1	EnCase	Succeed	12	OS, HV, Host, H/w, Net
1	FTK	Succeed	12	OS, HV, Host, H/w, Net
1	FTK Picture (disk)	Succeed	12	OS, HV, Host, H/w, Net
1	Fast dump	Succeed	2	OS, HV, Host, H/w, Net
1	memoryze	Succeed	2	OS, HV, Host, H/w, Net
1	FTK Picture (memory)	Succeed	2	OS, HV, Host, H/w, Net
1	Capacity Block Copy	Succeed	14	OS (imaging machine), HV, Host, H/w, Net
2	Agent Injection	Succeed	1	HV, Host, H/w, Net
3	AWS Distribute	**Succeed**	120	**AWS Engineer, Specialist's Host, H/w and Software,**

4. Encounters in Cloud Forensics

4.1. Data Acquisition

This is the first and most important stage of the process of forensics. Any fault in this phase is carried over to the ones that follow, changing the direction that the investigation takes. In the area of digital forensics, researchers take hold of the compromised computer (or other digital equipment) and use forensic methods to search for evidence of malicious behaviour, making sure that the data is not tampered with. However, because cloud computing is remote and multi-tenant, it is not practicable to seize the equipment in cloud forensics. As stated by Birk, there are three possible states for the evidence in the cloud: at rest, in motion, and in performance. Compared to conventional forensics, this will make data collecting more difficult. The following are a few of the difficulties the researchers encountered when trying to collect data in a cloud setting.

4.1.1. *Physical Inaccessibility*

Because of the important properties of clouds, evidence is dispersed and stored in various areas. This makes data collecting inaccessible and has an impact on the data capture procedure.

4.1.2. *Fewer Controller in Cloud*

In contrast to digital forensics, where the seizure of electronic devices is uncertain, cloud users and researchers have restricted access. This makes the process of acquiring data in a cloud environment more difficult. The cloud access control differs according to service types, as Fig. 3 illustrates. In the SaaS and PaaS formats, the agent can only access logs connected to the programme. Customers can create applications in PaaS to obtain specific additional forensics information, unlike in the SaaS model where access is severely restricted. Under the IaaS concept, users can advance to the operating system level. IaaS has been provided with greater rights than the other two models. Despite the fact that different levels of access restrictions are reachable in the cloud, forensic investigators must plan for data collection from Cloud Service Providers (CSPs). The data acquisition issue is cited by J. Dykstra and A. Sherman using a fictional case study involving child pornography. The warrant issue—that is, the requirement that the location be indicated in the warrant—has been addressed by the authors of this case study, despite the fact that the data is dispersed and kept in multiple cloud locations. Because cloud servers are multi-tenant, an investigator cannot seize a cloud server until it has arrived at the site. Service providers utilize virtual machines (VMs) to provision their clients. If this virtual machine (VM) is not matched by storage devices such as Amazon S3, volatile data such as registry accesses or impermanent internet files will be vanished. This means that at what time the VM is restarted or halt, all of its contents are lost.

4.1.4. *Trust Issue*

The reliance on a third party to gather evidence in the cloud is another major issue. After a search warrant was obtained, this problem was brought up in a child pornography prosecution. To help him gather data, the investigator requires internal workers. The truthfulness of the data to be twisted in court can sometimes be compromised by the fact that this individual is not a certified investigator or is from the same CSP. In cloud computing, multiple clients share separate resources under multi-tenancy. The investigator addresses two challenges when collecting evidence from the cloud. In command to preserve the honesty of the data belonging to other users, he must first demonstrate that the retrieved data has not been tampered with.

4.2. Logging

The initial stage in digital forensics is log analysis. The logs could be network, system, application, or process logs. Logging is the most important for the search process, but obtaining the cloud-based log data is also essential. The following are some of the difficulties that are identified when getting logs.

4.2.1. *Reorganization*
The logs in the cloud are dispersed during the network. This issue makes it more challenging for cloud investigators to compile logs from several sources.

4.2.2. *The Instability of Logs*
CSPs utilize virtual machines to deliver solutions to their clients. When a virtual machine (VM) is restarted or shut down, any information that is volatile, such as transient internet files and registry data, is lost forever.

4.2.3. *Accessibility of Logs*
The logs are utilized for debugging, troubleshooting, and other purposes, and there is no process or way to view them in other locations.

4.3. Necessity on CSP
Because the logs are gathered and kept on CSP property, users and investigators must rely on CSPs to gain access to server and network logs. Here's where CSP might meddle with logs.

4.4. Chain of Protection
The term "chain of protection" refers to the order in which a old item, file, or combination of papers have been owned, possessed by or located. It is evident from this, one of the most important forensic enquiry concerns, when and how the proof was gathered, examined, arranged, and delivered in court. Because digital forensics allows for the seizure of equipment, applying this process is simpler than it is in cloud forensics. This does not apply to cloud forensics due of the multi-jurisdictional regulations and processes involved. As a result, a chain of custody presents numerous difficulties for cloud forensics. Multiple users' access to evidence has been highlighted by J. Dykstra and A. Sherman in a fictional event learning of a corrupted cloud-based website. Thus, in order to obtain the chain of custody, investigators must rely on CSP. The dependability of hypervisor for a chain of protection was questioned by Birk et al.

4.5. Crime Act Rebuilding
Reconstructing a crime scene in a cloud environment is impossible because data in virtual machines (VMs) is permanently deleted when they are powered off or restarted.

4.6. Cross Border Law
The global distribution of data centers made possible by cloud providers means that cross-border law is a crucial problem for cloud forensics. While the methods for data protection and chain of protection vary depending on the panel, the examination process as a whole will be impacted through the cross-border law, the investigation process itself should be conducted in accordance with the laws of the particular jury.

4.7. Law Presentation
Digital and cloud forensics culminate in a jury trial presentation. Thousands of virtual machines (VMs) operate in cloud data cores, and couple of handlers can access them at once. This makes cloud forensics more difficult than digital forensics.

5. Proposed solution
The only sites where the before recognized answers can be used are cloud buildings, and agents must rely on CSP to get forensic evidence for their investigations. The suggested approach is put into practice off the cloud's premises in order to get around these restrictions. After getting approval from the (ITU), the endorsed key lectures the data gathering matters covered in the literature by familiarizing a unified forensic server and a forensic coat external the cloud organization acknowledged as the forensic monitoring plane (FMP). Thus, the agents do not have to rely on the CSP to gather information. Fig. 4.1 illustrates the suggested cloud forensics model, which includes the addition of forensic servers and the forensic monitoring plane (FMP) to advance cloud forensics. The entire incoming and outcoming connection in a cloud environment will be observed by forensic tools like the forensic toolkit (FTK) analyzer running at the topmost of the FMP. The monitored data is forensically pictured, or one step at a time stream encrypted, and is stored in a detached forensics server that is situated in a cybercrime site. The cloud service models' actions are also observed by the forensic tool. In cloud service models that involve virtual machines (VMs), the tool mechanically gathers a forensic picture of the existing state and stores it in a different forensics' server. In order to permit a decrease in the level of self-assurance on CSP, all actions, together with net traffic flow in the particular cloud, are forensically photographed on every instance a happening happens, or the invitation deal with in the cloud is obtained, encrypted again, and kept in the forensic server. Since by stage stream tomography is executed through the forensic picture, the data that is forensically photographed remains unchanged

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

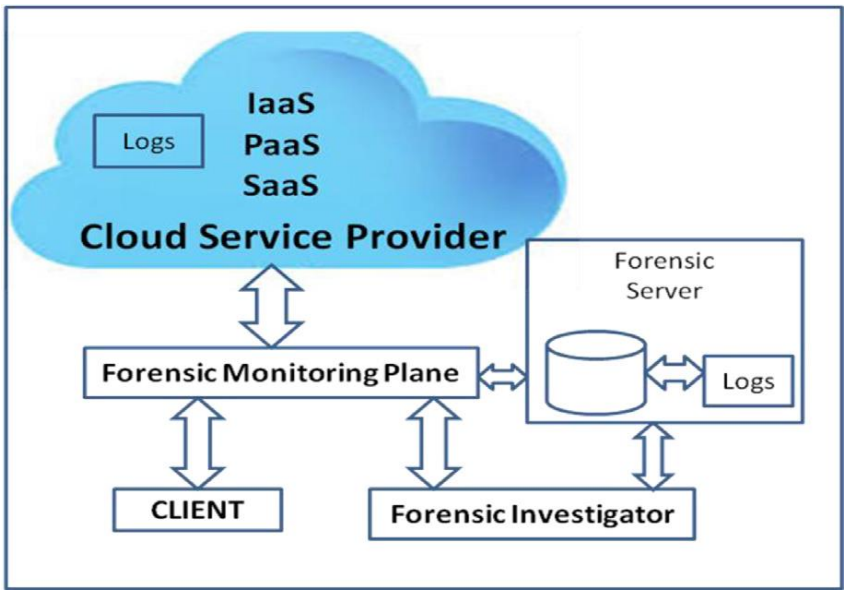

Fig. 5.1. Projected Model for Cloud Forensics

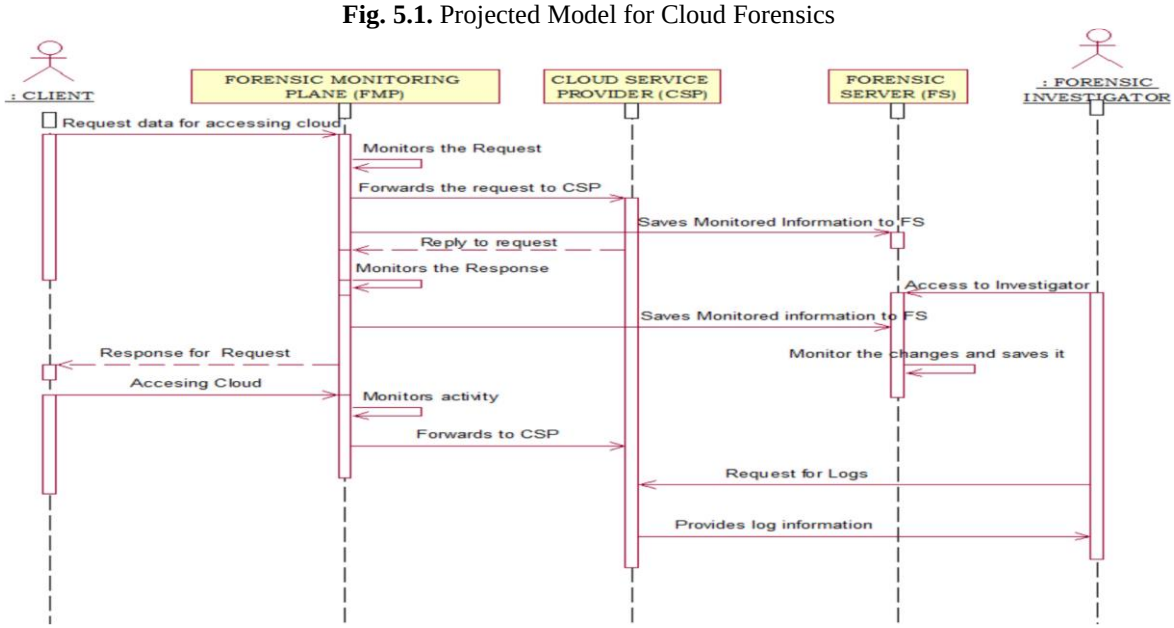

Fig. 5.2. Order Illustration for Planned Model.

development. The only tools available for processing the obtained forensic photos are forensics-related ones; they are not raw data. Additionally, network logs from nearby network devices—such as routers—are obtained and pictured in a forensics server to provide strong evidence against the attacker. If there is any malicious activity, the agents can get the forensic evidence within a certain time limit by logging in with their user credentials to the forensic server. In the meantime, in the event of suspicion, the investigator can ask CSP for information and cross-reference it with information gleaned from the forensic server. The forensic is using forensic tools.
server, and in the occasion of any unexpected happening, it retrieves the forensic picture of the server because there's a potential that a suspicious could log in as a forensic agent and alter the data. For better understanding, a categorization diagram is used in Fig. 4.2 to explain the order of operations in our suggested model. Dealings in the recommended model:
•The user starts the demand to the CSP.
•Criminalistic agent logs into the criminalistic server for studying the indication composed.
Additionally, actions taken within the criminalistic server are preserved and photographed forensically. The integrity of the data that has been gathered is also confirmed if the investigator starts asking the CSP for evidence bases and comparability them with one another in case he has suspicions about them. It is clear from the suggested solution that there is less reliance on CSP to obtain data. Storing log files centrally and separately also lessens the logging challenge. Cloud forensics will advance thanks to the newly proposed forensic model.

6.Conclusion

Cloud forensics are becoming more and more necessary as a result of cloud computing's explosive expansion and the potential for cloud-related crime to occur in the digital realm. Cloud forensics poses numerous issues, many of which have only been partially addressed by researchers. This paper provides a detailed overview of the difficulties experienced in cloud-based forensics and the explanations that the scholars have come up with. A fresh approach to addressing the difficulties in cloud forensics has been put forth, and its viability has been tested using a denial-of-service (DDoS) attack to see if the suggested FMP gathers all the data required to investigate fraudulent activity for forensic purposes. In the future, a cloud-based model will contain the full attack scenario.

We have shown that the most popular forensic tools available today are theoretically capable of remotely acquiring data from Amazon EC2. We have also demonstrated that technology is not enough to provide reliable data and resolve the cloud forensic collection issue because many levels of trust are needed. The four ideas we put forth give solutions that connect provider support with technology. The management plane is what we advise for the forensic acquisition of IaaS cloud computing. The most appealing mixture of control and speed with confidence is provided by this option. We have started a rollout to enable cloud providers to provide users with this kind of access to forensic data. Although EnCase and FTK were able to excellently return mark, we do not advise utilizing them for cloud-based remote forensics due to the high degree of trust that is needed. Future research is still needed in a few areas. Initially, we conducted IaaS-specific research with EC2. These findings are not applicable to additional cloud models and settings, analogous Google App Engine otherwise Microsoft Azure, someplace forensic application software cannot be deployed and operated in the same manner as it can in EC2. It will take more effort in the future to identify appropriate comparisons on those platforms. Second, the consumer-driven forensic capabilities that the cloud provider exposes to them would be advantageous to the users. Our goal is to collaborate with providers so that users may obtain metadata and forensic logs (such disc volume cryptographic checksums) straight from the online management console. Third, when cloud resources are released, measures must be taken to protect evidence and stop it from being lost. In conclusion, we intend to investigate acquisition law further in the future, especially as it relates to Fourth Amendment issues of jurisdiction, ownership, and search and seizure.

References

1) Amazon Web Services. AWS import/export. Available at: http://aws. amazon.com/importexport/; 2011.
2) Casey E. Digital evidence and computer crime: forensic science, computers, and the Internet. 2nd ed. Amsterdam: Elsevier Academic Press; 2004.
3) Conover M, Chiueh T. Code injection from the hypervisor: removing the need for in-guest agents. In: Proceedings of Blackhat USA; 2008.
4) Dolan-Gabitt B, Payne B, Lee W. Leveraging forensic tools for virtual machine introspection. Technical Report, Georgia Institute of Technology, GT-CS-11-05; 2011.
5) Dykstra J, Sherman AT. Understanding issues in cloud forensics: two hypothetical case studies. In: Proceedings of the 2011 ADFSL conference on digital forensics security and law. ASDFL; 2011a. p. 191–206.
6) Dykstra J, Sherman AT. Understanding issues in cloud forensics: two hypothetical case studies. Journal of Network Forensics 2011b;3(1):19–31. Eucalyptus. Eucalyptus: the open-source cloud platform. Available at: http://open.eucalyptus.com/; 2011
7) Federal CIO Council. Guidelines for the secure use of cloud computing by federal departments and agencies (draft version 0.41); 2011.
8) Garfinkel S. Forensic feature extraction and cross-drive analysis. Digital Investigation 2006; 3:71–81.
9) Garfinkel T, Rosenblum M. A virtual machine introspection-based architecture for intrusion detection. In: Proceedings of the 10th annual symposium on Network and Distributed System Security (NDSS 2003); 2003. p. 191–206.
10) Giobbi R, McCormick J. Vulnerability Note VU#912593: Guidance EnCase Enterprise uses weak authentication to identify target machines. Available at: http://www.kb.cert.org/vuls/id/912593; 2007.
11) Guidance Software. EnCase Legal Journal. Available at: http://www. guidancesoftware.com/DocumentRegistration.aspx? did¼1000017380; 2011.
12) Heiser J. Remote forensics software. Gartner RAS Core Research Note G00171898; 2009.
13) Krautheim FJ. Building trust into utility cloud computing. Ph.D. thesis; Department of Electrical Engineering and Computer Science, University of Maryland, Baltimore County; Baltimore, Maryland; 2010.
14) Krautheim FJ, Phatak DS, Sherman AT. Trusted virtual environment module: managing trust in cloud computing. In: 3rd international conference on trust and trustworthy computing; 2010. p. 211–27. Lib VMI. Virtual Machine Introspection (VMI) tools. Available at: http:// vmitools.sandia.gov/; 2011.
15) Nance K, Hay B, Bishop M. Investigating the implications of virtual machine introspection for digital forensics. In: Proceedings of the international conference on Availability, Reliability and Security (ARES '09); 2009. p. 1024–9.
16) National Institute of Standards and Technology. Computer forensic tool testing (CFTT) project overview. Available at: http://www.cftt.nist. gov/project_overview.htm; 2003.

17) National Institute of Standards and Technology. Digital data acquisition tool specification. Available at: http://www.cftt.nist.gov/Pub-Draft-1- DDA-Require.pdf; 2004.
18) National Institute of Standards and Technology. Test results for digital data acquisition tool: FTK picture 2.5.3.14. Available at: http://www. ncjrs.gov/pdffiles1/nij/222982.pdf; 2008.
19) National Institute of Standards and Technology. Test results for digital data acquisition tool: EnCase 6.5. Available at: http://www.ncjrs.gov/ pdffiles1/nij/228226.pdf; 2009.
20) National Institute of Standards and Technology. The NIST definition of cloud computing. Available at: http://csrc.nist.gov/publications/ nistpubs/800-145/SP800-145.pdf; 2011.
21) Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics: an overview. In: Advances in digital forensics VII; 2011.
22) Santana M. Cloud security: beyond the buzz. Available at: http://www. linuxworldexpo.com/storage/10/documents/CI7%20Mario% 20Santana.pdf; 2009.
23) Santos N, Gummadi K, Rodrigues R. Towards trusted cloud computing. In: Proceedings of USENIX HotCloud. Available at: http://static.usenix. org/events/hotcloud09/tech/fullpapers/santos.pdf; 2009.
24) Sato H, Kanai A, Tanimoto S. A cloud trust model in a security aware cloud. In: Proceedings of the 2010 10th IEEE/IPSJ international symposium on applications and the Internet. SAINT '10; 2010. p. 121–4. SCMagazine. Best computer forensic tool. SCMagazine; 2011.
25) Shields C, Frieder O, Maloo M. A system for the proactive, continuous, and efficient collection of digital forensic evidence. In: The proceedings of the eleventh annual DFRWS conference, vol. 8; 2011. p. S3–13.
26) Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Network Security 2011;2011(3):4–10.
27) Terremark. Secure information services. Available at: http://www. terremark.com/uploadedFiles/Services/Security_Services/TMRK_SIS_Gatefold2_4pagelayout_Screen.pdf; 2009 [accessed 01.11.11].
28) United States Code. Communications Assistance for Law Enforcement Act (CALEA). 47 USC 1001-1010; 1994.