Chapter 6

Cloud Forensic

Cloud computing is a computing platform which provides everything as a service to the user in the digital world. Security is one of the deepest concerns in the cloud environment. Cloud forensics is the process of investigating and analyzing cloud security threats. In this chapter, cloud forensics is discussed along with challenges and research directions.

Cloud forensics is the application of digital forensic science in the cloud computing environment as a part of network forensics. In other terms, cloud forensics is the cross-discipline between cloud computing and digital forensics. As cloud computing is part of network, cloud forensics can also be considered as a subset of network forensics.

Three Dimensions of Cloud Forensics:

Cloud forensics is not just a technical issue but, a multi-dimensional issue. In this chapter we will study all the three dimension characteristics of cloud forensics- Technical dimension, Organizational dimension and legal dimension

A) Technical Dimension : It consist of tools and procedures that are required to perform the forensic investigation in cloud computing environment.

1. Data Collection: This process include the following steps: identifying, labeling, recording and acquiring forensic data. The forensic data includes artifacts from the customer's end that reside on customer premises and the artifacts from service provider's end that are located in the cloud service provider infrastructure

Segregation of duties between service providers and customers in forensic responsibilities become different in different service models, and interaction between multi-tenants sharing same resources are different in different deployment models. The collection process should preserve the integrity of data with clearly defined segregation of duties between the customer and service provider. It should also follow the chain of custody throughout the investigation process.

2. Challenges: s. In every combination of cloud service model, the cloud customer faces the challenge of decreased access to data. Access to data varies considerably based on the cloud model that is implemented. Cloud customers generally have little or no control of the physical locations of their data.

Service providers intentionally hide data locations from customers to facilitate data movement and replication. For example, we require IP logs, virtual machine access logs and disk images in data collection process, all this information is crucial while conducting the investigation, but it is very difficult to gather these information from cloud servers.

3.Data storage Elasticity: It is considered to be one of the central attributes to cloud computing. Elasticity plays a major role in cost reduction. The cloud resources can be provisioned and released quickly on demand. Also, the resource acquiring and releasing can be automated to make sure that the application requiring the resource will have that resource at any given point of time

a)Proliferation of Endpoints: the large number of resources connected to the cloud, the impact of a crime and the workload of an investigation can be massive.

b) Event-time synchronization: Time synchronization of events is complicated because the data of interest resides on multiple physical machines in multiple geographical regions, or the data may be in transit. Thus, making it difficult for the forensics expert to study the series of events taking place before the intrusion.

c) Retrieve deleted data: Deleted data is an important source of evidence in traditional digital forensics.

In the cloud, the customer who created a data volume often maintains the right to alter it. When the customer deletes a data item, the removal of the mapping in the domain begins immediately and is typically completed in seconds. Remote access to the deleted data is not possible without the mapping.

3.Virtualization: The capability of cloud to provide multi-tenant services at the infrastructure, platform, or software level is often justified by the ability to provide some form of virtualization to create economic scale. It is a key technology that is used to implement cloud services. If Virtual Machine (VM) technology is used in cloud infrastructure, then we must be concerned about compartmentalization and hardening of those Virtual Machines.

Many cloud service providers' uses hypervisor to monitor and run the servers. Hypervisor is used to control and monitor the virtual cloud server without actually going to the physical location of the servers.

It is always easy to attack main system rather than attacking multiple systems of interest. This logic is applied by the attackers and they usually try to attack the hypervisor. Hypervisor can be compared as the kernel of the old operating system. Due to lack of policies, procedures, tools and techniques it is very difficult for the forensic investigator to investigate the hacked hypervisor and gather the important information.

4. Proactive preparation : Proactive measures are often taken as preparation to create forensic investigation easier. Due to this embrace planning forensics aware cloud application and proactively assembling forensic knowledge within cloud victimization tools provided by CSP or tools developed from client aspects.

5. Evidence Segregation : Cloud forensics includes the contrary process of evidence separation but underlying components that make up the cloud substructure such as CPU caches , GPU. They produces to separate forensic data among multiple tenants in cloud deployments.

Organization Dimension of Cloud Forensics

Forensic investigation in cloud computing environment involves three entities, these being- consumer, cloud service provider, and sometimes the third party. Proper organizational structure is required in order to carry out cloud forensic activities flawlessly and effectively. Organizational structure will help us in understanding the set of rules that should be followed inside the organization in order to secure the cloud data. It is very important for any organization to secure their systems from internal attacks. Most of the time internal attacks are occurring due to ignorance of the internal staffs. Also, internal staff, customers and external assistant should be trained enough to help the forensic investigators.

1. External Dependency chains: We have studied about third parties involving in cloud services. Many a times there are more than 3 cloud service providers involved in providing the service (based on the location). This shows that one CSP is having dependencies over other CSPs. A cloud forensic investigation thus requires investigations of each individual link in the dependency chain. Correlation of the activities across CSPs is a major challenge. Lack of coordination between the CSPs involved can lead to problems. Due to the lack of procedures, policies and agreements related to cross-provider forensic investigations it is very difficult for the forensic team to investigate when multiple CSPs are involved

2. Investigators : The main task of investigation is cooperative investigation allegations of misconduct within the cloud. They must have sufficient expertise to perform investigation of their own set of tools as well as interact with other security agencies in forensics investigations.

3. IT professional : They perform data collection with help of technical expertize in network, security and system administration.

4. Incident Handlers : They deals with accidental data leakage , unauthorized data access and data loss, breach of tenant confidentiality, malicious code infection, malicious insider attack, denial of service attack and inappropriate system usage.

5. External assistance : Cloud Service Provider sometimes collaborate internal employee with external parties to perform forensics task like e-discovery , investigation on civil cases and investigation on external chain of dependencies. In this case cloud organization need to work closely with law enforcement to improve mutual understanding and collaborate much further in case of resource confiscation. Also involve third party forensics auditor and cloud academia to get new up to date knowledge and research in cloud data.

Legal Dimension in Cloud Forensics

The legal dimension of cloud forensics defines the policies and service level agreements to ensure that forensic activities do not breach laws and regulations in the jurisdictions where the data resides. It should include the policies and procedures that are common and applicable in all the tenants where the data are accessed and stored. This means, the confidentiality of other tenants that share the same infrastructure should be preserved. SLAs define the terms of use between a CSP and its customers.

The Rules and regulation between Service Level Agreement and Cloud Client as follows:

a)The services, techniques supported and accesses provided by the CSP to customers during forensic investigations.

b) Trusted boundaries, roles and responsibilities between the service providers and customers regarding forensic investigations.

c) The process for conducting investigations in multi-jurisdictional environments without violating the applicable laws, regulations, and customer confidentiality and privacy policies.

d) Legal challenges include identifying and addressing issues of jurisdictions for legal access of data; lack of effective channels for international communication and cooperation during an investigation, multi-tenant jurisdiction and missing terms in contracts and service level agreements.

e) Service Level Agreement (SLA): Transparency in the SLA creates the biggest challenge for the forensic investigators. Due to unawareness in the customers, non- transparency between CSPs and lack of international laws and regulations, SLAs are not prepared properly by the CSP and this creates the loop hole in the investigation process.

f) Multiple Jurisdiction and Tenancy: Laws and regulation differs from country to country or even part of country and multiple tenancy is the biggest characteristics of cloud computing. Customers can be connected to the cloud server from different locations. The absence of a worldwide regulatory body or even a federation of national bodies significantly affects the cloud forensic investigations

Usage of Cloud Forensics

1. Investigation :

a) Investigation on policy violation cloud crime in a multitenant and multijuridictional cloud environment.

b) Provides admissible evidence to the court.

c) Collaboration with law enforcement in resource confiscation

d) Event reconstruction in the cloud.

e) Collaboration with law enforcement in resource confiscation.

2. Troubleshooting :

a) To build new policies to help reappearance of similar events and to regulate the original reasons

For solitary events or styles spanning multiple actions over time.

b) Map out an event and evaluating the present state of an event in the cloud.

c) Security Event handling in the cloud.

d) Resolving purposeful matters in cloud applications and cloud services.

e) Resolves working issues in cloud systems.

f) Pinpointing hosts and data files virtually and actually in cloud environments.

3. **Legal Monitoring :** Analyzing,collecting and correlating log entities across multiple systems in the cloud assisting in auditing, regulatory compliance and other efforts due diligence.

4. Data and system recovery :

a) Recovering data in the cloud that has been intentionally modified or deleted.
b) Recovering systems from accidental attacks or damages
c) Recovering encrypted data in the cloud when the encryption key has been lost.
d) Acquiring data from the cloud that are being redeployed, retired or need to be sanitized.

5. Due diligence / regulatory compliance :

Helping organization exercise due diligence and comply with requirements such as protecting sensitive information, maintaining certain records for notifying impacted parties, audit purpose when protected information is exposed and more.

Interaction of Email system with local and cloud storage

Mail can still be useful as a method of sharing files with others, but it is now in direct competition with cloud storage and collaboration service offerings. For example, Google Drive and Evernote allow their users to share documents and files without directly attaching those files to an email. A simple URL link is all that is needed for a group to easily initiate collaboration on the same document. In theory, email is more private because it's not broadcasting the data for all to see, the way social networks do, but social networks are aware of users' transient need for privacy.

These services are Internet-based, meaning that if you can connect to the Internet, you can access these tools. If your Internet connection goes out at the office, you lose access to your email. If you have your own server and lose access to the Internet, you still lose the ability to email. When you consider the cost of a cloud-based email service, make sure to consider all of the costs involved in maintaining your own server in-house.

These types of email server services require no hardware on your part. In fact, there is typically no software required, except for perhaps an Internet browser or email client. Google has an inexpensive service that can do that, and so does Microsoft. And you'll get email addresses @yourdomain.com. Many website hosting services such as GoDaddy also provide professional email-hosting services that allow you to use @yourdomain.com.