Unit-6

Cloud Forensics

Contents

- Fundamentals of cloud forensics
- Cloud crimes
- Uses of cloud forensics and its challenges
- Interaction of Email system with local and cloud storage

Fundamentals of cloud forensics

- Cloud computing is game-changing technology.
- Cloud computing does not have process that allows a set procedure on how investigate or issue about cloud.
- we have define cloud forensics and analyze its challenges and opportunities.
- Cloud computing is the new era of rapidly growth information and communication technology world.
- Cloud computing service provide on third growth of overall IT industry
- The rise of field has demanded to gain new knowledge for digital forensic investigators.
- Investigators should have knowledge, practice and command on tools working in cloud computing environment help cloud organizations, including both CSP(cloud service provider) and cloud customers to reduce cloud security risk and secure data.

- 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.
- Cloud forensics follow the main principles found in the network forensic process with some techniques specially customized for the cloud computing environment

Why do we need Cloud Forensics?

- The demand of cloud computing is increasing exponentially.
- As per the Forbes report, IT companies spending on security technologies will increase 46% by next year, with cloud computing increasing 42% and business analytics investments is up by 38%.
- Thus, as the year passes the demand of cloud will be increasing.
- Although cloud computing has become increasingly popular, security remains a vital concern when accessing data online.
- The cloud service providers and the customers have yet to establish forensic capabilities that will support the investigation in case if any crime is committed.

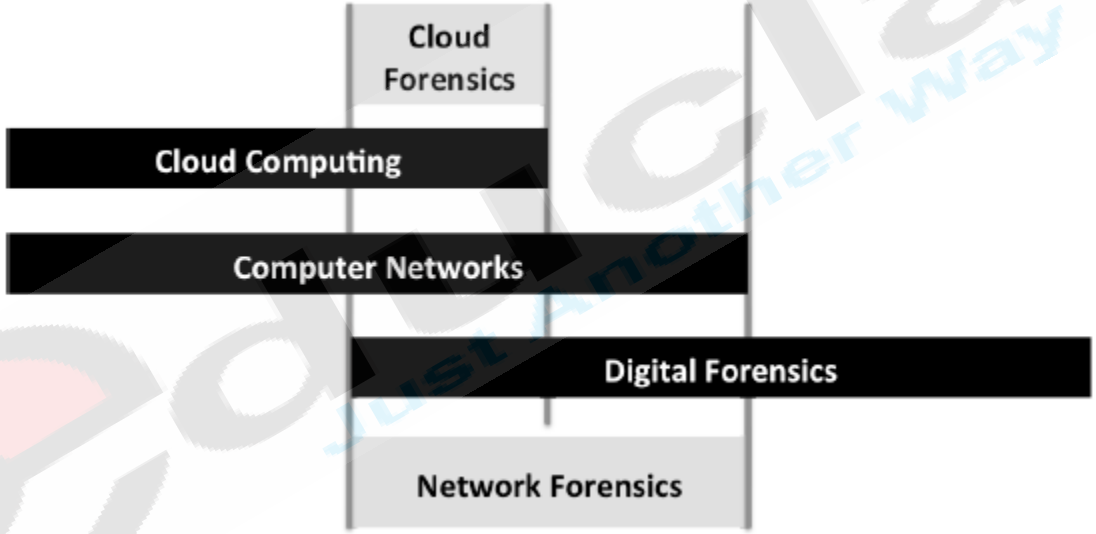
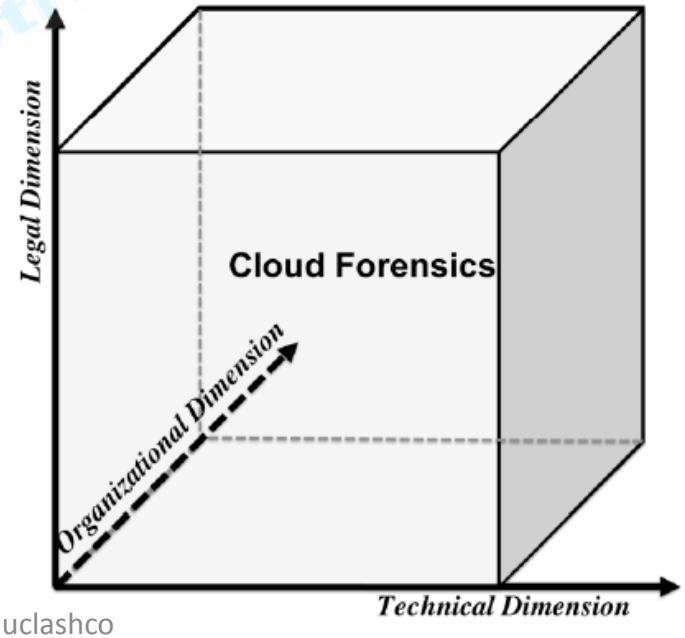


Fig1 Cloud Forensic

Three dimensions of cloud forensics

- We can extend the definition of cloud forensics across three major dimensions;
  - Technical dimension
  - Organizational dimension
  - Legal dimension



- **Technical Dimension:**
  - The technical dimension involves a set of tools and procedures to carry out the forensic process in cloud computing environments
  - Some of the key aspects in the technical dimension as follows:

1. Evidence segregation

  - Another essential characteristic of cloud computing is resource pooling(describe a situation in which providers serve multiple clients, customers or "tenants" with provisional and scalable services).
  - IT cost is reduced in multi-tenant environments where various resources are shared.
  - Cloud forensics involves the reverse process of evidence segregation, but the underlying components that make up the cloud infrastructure, e.g., CPU (Central Processing Unit) caches, GPU (Graphics Processing Units), etc., were not designed for strong compartmentalization in a multi-tenant architecture
  - Tools and procedures to segregate forensic data in the cloud among multiple tenants in different deployment models and different service models need to be developed.

2. Forensic data collection:

- Cloud forensic collection is the process of identifying, labelling, recording, and acquiring forensic data from the possible sources of data in the Cloud.
- These data sources include client-side artifacts that reside on client premises, and provider-side artifacts reside on provider infrastructure.
- Different cloud service models, the tools and procedures to collect forensic data are also different.
- Provider-side artifacts are different, e.g., in public clouds, provider-side artifacts need to be segregated among multiple tenants, whereas in private clouds, there is no such need.
- The sequence order in which data is collected is defined according to the volatility of data; highly volatile data (i.e. RAM images) should be collected first, followed by data with lower volatility.
- The collection process should follow procedures that preserve the integrity of data, with clearly-defined segregation of duties between client and provider, and without breaching law and regulation under the jurisdiction where data is collected, or compromising confidentiality of any other tenant(s) sharing the same resource(s).

3. Elastic, static and live forensics

- Rapid elasticity is one of the essential characteristics of cloud computing.
- Cloud compute and storage resources can be provisioned and deprovisioned on demand.
- As a result, cloud investigation tools also need to be elastic; in most cases large scale static and live forensic tools are required, such as e-discovery, data acquisition, data recovery, evidence examination, evidence analysis tools and tools to collect volatile data

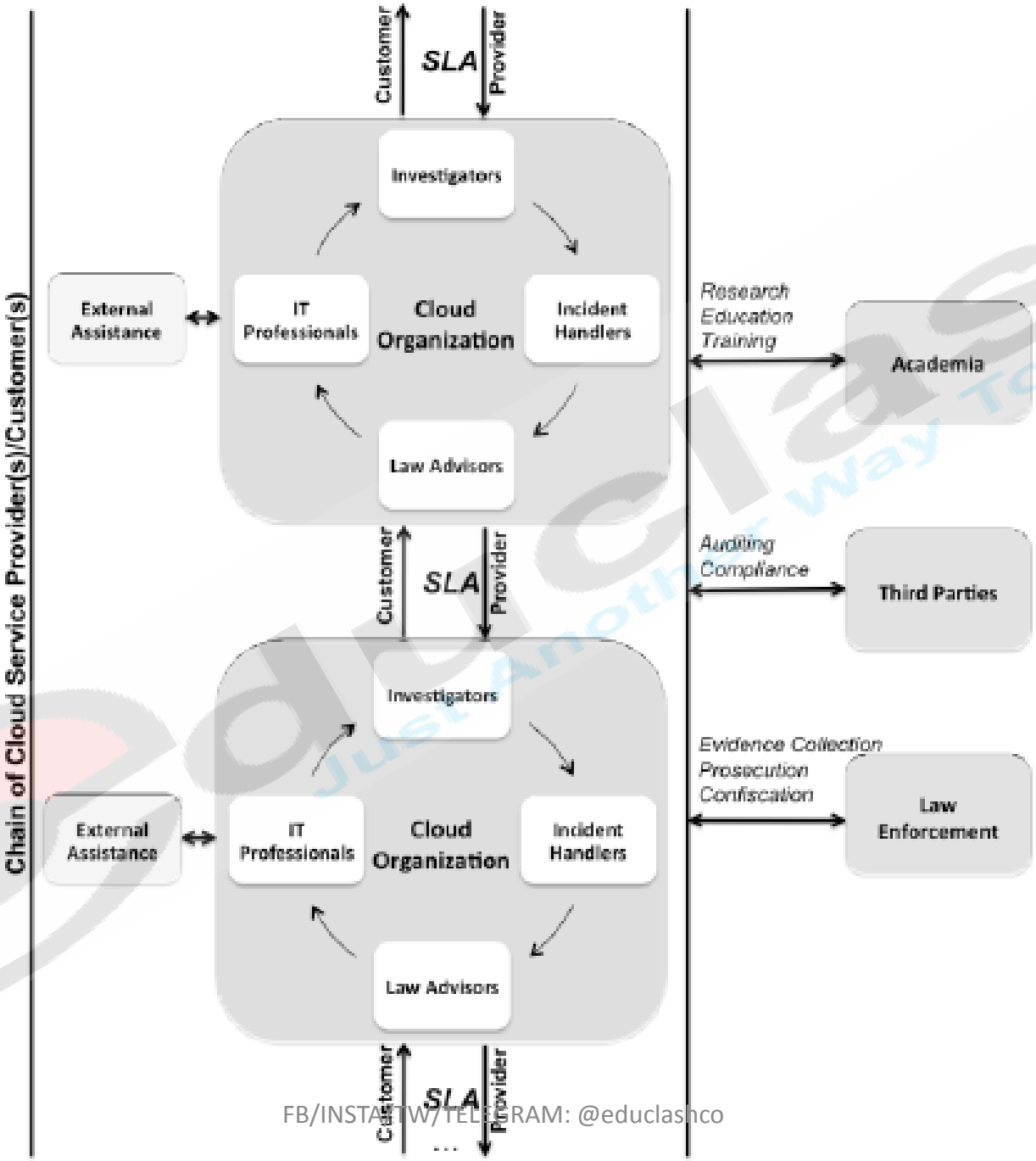
4. Investigations in virtualized environments

- Virtualization is a key technology used to implement cloud services.
- Tools and procedures are yet to be developed for investigations in virtualized environment, e.g. hypervisor investigations.
- On the other hand, while operations are mostly virtualized in cloud environments, investigations in most cases require evidence retrieval from physical locations.
- Loss of data control is one of the major security challenges in the Cloud .
- In cloud forensics, tools and procedures need to be developed to physically locate forensic data at a given timestamp, and physically trace forensic data at a given time period, taking into considerations of the jurisdiction(s) of the physical locations

5. Pro-active preparations

- Pro-active measures can be taken as preparations to make forensic investigation easier. Such measures include designing forensic-aware cloud applications, and pro-actively collecting forensic data in the Cloud using tools provided by the CSP or tools developed from the customer side.
- It involves a set of design principles, such as conducting regular snapshots to remote storage, regularly tracking authentication and access-control records and performing object-level auditing of all access

- **The organizational dimension**
- Forensic investigations in cloud computing environments always involves at least two parties: the CSP(cloud service provider) and the cloud customer.
- When the CSP outsources services to other parties, the scope of investigation widens.
- Figure shows the proposed organizational structure needed in order to carry out cloud forensic activities efficiently and effectively with a joint effort



- **Organizational structure for each cloud organization:**
  - Establish a forensic capability, each cloud organization, including the providers and customers of cloud services, is required to define a structure of internal staffing, provider-customer collaboration, and external assistance fulfilling the following roles:

1. Investigators:

- Investigators (on the provider side and on the customer side) are responsible for collaborative investigation allegations of misconduct in the Cloud and working with external assistance or law enforcement when needed.
- They not only need knowledge of how to carry out investigations from their own sides, but also need to understand the forensic capabilities of the parties they are interacting with and the segregation of duties among these parties regarding forensic investigation.

2. IT Professionals:

- This group includes system, network, and security administrators, ethical hackers, cloud security architect, and technical support staff in the cloud organization.
- They contribute to the investigation with their expertise, facilitate the investigators in accessing the crime scene, and may also perform data collection for the investigators.

3. Incident Handlers:

- This group responds to a variety of specific security incidents in the Cloud, such as unauthorized data access, accidental data leakage and data loss, breach of tenant confidentiality, inappropriate system usage, malicious code infections, malicious insider attack, (distributed) denial of service sttacks, etc.

4. Legal Advisors:

- It is crucial to include legal advisors in forensic staffing who are familiar with multi-jurisdiction and multi-tenant issues in the Cloud so that any forensic activities will not violate regulations under respective jurisdiction or confidentialities of other tenant sharing the same resource.
- Service Level Agreements (SLAs) must be written with clauses that explain the procedures to follow in the event of a forensic investigation.
- An internal legal advisor should be involved in drafting these clauses so that they respect the law across all jurisdictions in which the CSP operates.
- Internal legal advisors are also responsible to communicate and collaborate with external law enforcement during the course of a forensic investigation.

5. **External Assistance:**

- cloud organizations to rely on a combination of its own staff and external parties to perform forensic tasks such as e-discovery, investigations on civil cases, investigations on external chain of dependencies.
- It is important for cloud organizations to determine in advance, which actions should be performed by external assistance regarding forensic activities, and make it clear in relevant policies, guidelines and agreements which are transparent to its service customers and law enforcement when necessary.

- **Chain of Dependencies:**
- CSPs and most cloud applications often have dependencies on other CSP(s).
- The dependencies in a chain of CSP/customer can be highly dynamic
- Any interruption or corruption in the chain or a lack of coordination of responsibilities between all the parties involved can lead to problems.
- Essential communications and collaborations regarding forensic activities through this chain need to be facilitated by organizational policies and legally binded in the SLAs.
- Consider following parties in order to facilitate effective and efficient forensic activities:

1. Law enforcement:

- Top priority for cloud organizations is the availability of service and the top priority for law enforcement is the prosecution of criminals .
- These two different priorities often clash in situations such as evidence collection.
- Cloud organizations need to work closely with law enforcement to improve mutual understanding, and collaborate much further in the cases such as resource confiscation.

2. Third parties:

- cloud organizations need to work closely with third parties for auditing and compliance purposes regarding cloud forensics.

3. Academia:

- cloud organizations need to work closely with academia on cloud forensic research and education in order to contribute to the knowledge of the area, and also to receive up-to-date training for their internal forensic staff.

- **The legal dimension:**
- **Multi-jurisdiction and multi-tenancy**
  - Multi-jurisdiction and multi-tenancy challenges have been identified as the top legal concerns among digital forensics experts and these two issues are both exacerbated in the Cloud.
  - Regulations and agreements have to be developed in the legal dimension of cloud forensics, to secure that forensic activities will not breach any laws or regulations under any jurisdiction where the data resides in, and the confidentiality of other tenants sharing the same infrastructure will not be compromised, throughout the investigation
- **Service Level Agreement**
  - SLA defines the terms of use between a pair of CSP and cloud customer.
  - The following terms regarding forensic investigations are not in place at the moment and have to be included into the SLA.

(1) Service provided, techniques supported, access granted by the CSP to the customer regarding forensic investigation

(2) Trust boundaries, roles and responsibilities between the CSP and the cloud customer regarding forensic investigation

(3) How forensic investigations are secured in a multi-jurisdictional environment in terms of legal regulations, confidentiality of customer data, and privacy policies

(4) How forensic investigations are secured in a multi-tenant environment in terms of legal regulations, confidentiality of customer data and privacy policies

Cloud crime

- Cloud crime is any crime that involves cloud computing.
- The Cloud can be the object, subject or tool of crimes.
- The Cloud is the object of the crime when the CSP is the target of the crime and is directly affected by the criminal act, e.g. DDOS (Distributed Denial of Service) attacks targeting part of the Cloud or even the entire cloud.
- The Cloud is the subject of the crime when it is the environment where the crime is committed, e.g., unauthorized modification or deletion of data residing in the Cloud, identity theft of users of the Cloud.
- The Cloud can also be the tool used to conduct or plan a crime, e.g., evidence related to the crime can be stored and shared in the Cloud and a Cloud that is used to attack other Clouds is called a dark Cloud.

Usage of cloud forensics

- There are various usages of cloud forensics. We summarize them as follows:

(1) Investigation

- Investigation on cloud crime and policy violation in multi jurisdictional and multi-tenant cloud environments
- Investigation on suspect transactions, operations and systems in the Cloud for incident response
- Event reconstruction in the Cloud
- Providing admissible evidence to the court
- Collaboration with law enforcement in resource confiscation

(2) Troubleshooting

- Locating data file and hosts virtually and physically in cloud environments.
- To determine the root cause for single events or trends spanning multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.
- Tracing an event and assessing the current state of an event in the Cloud
- Resolving functional issues in cloud applications and cloud services
- Resolving operational issues in cloud systems
- Security incident handling in the Cloud

(3) Log Monitoring

- Collecting, analyzing and correlating log entries across multiple systems in the Cloud, assisting in auditing, due diligence, regulatory compliance and other efforts

(4) Data and System Recovery

- Recovering data in the Cloud, that has been accidentally or intentionally deleted or modified
- Recovering encrypted data in the Cloud, when the encryption key has been lost.
- Recovering systems from accidental damage or attacks
- Acquiring data from the Cloud that are being redeployed, retired or need to be sanitized

(5) Due Diligence/Regulatory Compliance

- Helping organizations exercise due diligence and comply with requirements such as protecting sensitive information, maintaining certain records for audit purposes, notifying impacted parties when protected information is exposed, etc.

Challenges of cloud computing

- To establish a forensic capability for cloud organizations in all three-dimensions defined above, we are facing enormous challenges.
- In the technical dimension, we have very limited tools and procedures in all five major components that we emphasize in this paper.
- In the legal dimension there is currently no agreement among cloud organizations on collaborative investigation, and no terms and conditions are present in SLAs on segregation of duties between CSP and cloud customer.
- International cyber law and policies must progress to help resolve the issues surrounding multi-jurisdiction investigations

Challenges in forensic data collection

- In all combinations of cloud service and deployment models, the cloud customer faces the challenge of decreased access to forensic data.
- Access to forensic data varies dependent on the cloud model; IaaS customers enjoy relatively easy access to all data required for a forensic investigation, while SaaS customers may have little to no access to data required.
- Decreased access to forensic data means the cloud customer generally has no control or knowledge over the exact physical location of their data, and may only be able to specify location at a higher evel of abstraction, typically as an object or container identified.
- CSPs intentionally hide the location of data from customers to facilitate data movement and replication.
- There is a lack of appropriate terms of use in the SLA (Service Level Agreement) to enable general forensic readiness in the Cloud.
- Many CSPs do not provide services or interfaces for the customers to gather forensic data.
- For example, SaaS (Software as a Service) providers may not provide access to the IP logs of clients accessing content; IaaS (Infrastructure as a Service) providers may not provide forensic data such as recent VM (Virtual Machine) and disk images.
- In the Cloud, the customers have decreased access to relevant log files and metadata in all levels as well as a limited ability to audit the operations of the network of their CSP and conduct real-time monitoring on their own networks.

Challenges in elastic, static and live forensics

- The proliferation of endpoints, especially mobile endpoints, is a challenge for data discovery and evidence collection.
- The impact of crimes and the workload of investigation can be exacerbated in cloud computing simply because of the sheer number of resources connected to the Cloud.
- Time synchronization is crucial to the audit logs that are used as source of evidence in the investigation.
- Accurate time synchronization has been always an issue in network forensics, and is made all the more challenging in a cloud environment as timestamps must be synchronized across multiple physical machines spread in multiple geographical regions, between cloud infrastructure and remote web clients including numerous end points.
- Similar to time synchronization, unification of log formats has been a traditional issue in network forensics and the challenge is exacerbated in the Cloud because it is extremely difficult to unify the log formats or make them convertible to each other from the massive resources available in the Cloud.
- Proprietary or unusual log formats of one party can become major roadblocks in joint investigations.
- In computer forensics, recovered deleted data is an important source of evidence, so it is in the
- Cloud.
- In AWS (Amazon Web Service) the right to alter or delete the original snapshot is explicitly reserved for the AWS account that created the volume.
- When item and attribute data are deleted within a domain, removal of the mapping within the domain starts immediately, and is also generally complete within seconds. Once the mapping is removed, there is no remote access to the deleted data.
- Storage space occupied by the data elements deleted is made available for future write operations and the it is likely that storage space will be overwritten by newly stored data.
- Deleted data might be still present in the snapshot after deletion.
- A simple challenge is: how to recover deleted data, identify the ownership of deleted data, and use deleted data as sources of event reconstruction in the Cloud?

Challenges in evidence segregation

- In the Cloud, different instances running on the same physical machine are logically isolated from each other via hypervisor.
- An instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts.
- Customer instances have no access to raw disk devices, but instead are presented with virtualized disks.
- On the physical level system audit logs of shared resources and other forensic data are shared among multiple tenants. Currently, the provisioning and de-provisioning technologies still need to be much improved in the Cloud and it remains a challenge for the CSP and law enforcement to keep the same segregating in the whole process of investigation without breaching the confidentiality of other tenants sharing the same infrastructure and ensure the admissibility of the evidence.
- Another issue is that the easy-to-use feature of cloud models results in a weak registration system, facilitating anonymity that is easy to be abused and making it easier for cloud criminals to conceal their identities and harder for investigators to identify and trace suspects as well as segregate evidence.
- Encryption is used in the Cloud to separate data hosting of the CSPs and data usage of the cloud customers and most of the major CSPs encourage customers to encrypt their sensitive data before uploading to the Cloud if encryption is not provided by the CSP by default (Amazon, 2010; Force.com, 2010; Google, 2010).
- Unencrypted data in the Cloud can be considered lost from a strict security perspective. A chain of separation is required to segregate key management from the CSP hosting the data and needs to be standardized in contract language.
- Agreement has to be made among the law enforcement, the cloud customer and the CSP on granting access to keys of forensic data, otherwise evidence can be easily compromised when encryption key is destroyed.

Challenges in virtualized environments

- Cloud computing claims to provide data and compute redundancy by replicating and distributing
- resources.
- However in reality most CSPs implement instances of a cloud computer environment in a virtualized environment.
- Instances of servers run as virtual machines, monitored and provisioned by a hypervisor. The hypervisor in a Cloud is analogous to a kernel in the traditional operating system. Attackers will aim to focus their attacks against the hypervisor; compromise of the hypervisor amplifies any attack as many compute resources rely on its security.
- For law enforcement and cloud investigators, however, there is a huge lack of policies, procedures and techniques on hypervisor level to facilitate investigation.
- In the Cloud, mirroring data for delivery by edge networks, its redundant storage in multiple jurisdictions and the lack of transparent real-time information about where data is stored introduces difficulties for investigation. Investigators may unknowingly violate regulations, especially if clear information is not provided about the jurisdiction of storage.
- The CSPs cannot provide tools for the customer to locate at a given time, or trace at a given period of time, precisely and physically the multiple locations of a piece of data across all the geographical regions where the Cloud resides.
- Distributed nature of cloud computing forces a stronger international collaboration between law enforcement and industry, in cases such as confiscating “a Cloud” since the agency of a single nation cannot manage it when the physical servers are spread across different countries.

Challenges in internal staffing

- Today most cloud organizations are dealing with investigations with traditional network forensic tools and staffing, or are simply neglecting the issue.
- The major challenge in establishing a cloud forensic organizational structure is the lack of forensic expertise and relevant legal experience.
- The deep-rooted reasons for this challenge, which is also a challenge for the whole discipline of digital forensics, are firstly, the relative slow progress of forensic research compare to the rapidly evolving technology and secondly, the slow progress of relevant laws and international regulations.
- With only a decade of research and development, the discipline of digital forensics is still in its infancy, new forensic research areas in non-standard systems , such as cloud computing, need to be explored, techniques need to be developed, regulations need to catch up, law advisors need to be trained, staff need to be equipped with new knowledge and skills to deal with the new grounds for cyber crimes created by the rapid rise of new models such as cloud computing.

Challenges in external chain of dependency

- CSPs and most cloud applications often have dependencies on other CSPs. For example, a CSP providing an email application (SaaS) may depend on a 3rd party provider to host log-files (PaaS), who in turn may rely on a partner to provide infrastructure to store log files (IaaS).
- Many predict the industry is moving towards federated or integrated Cloud in the near future, today every CSP has a different approach to solving this problem.
- Correlation of activities across CSPs is a big challenge.
- Investigation in the chain of dependencies between CSPs may depend on the investigations of each
- one of the links in the chain and level of complexity of the dependencies.
- Any interruption or corruption in the chain or a lack of coordination of responsibilities between all the parties involved can lead to problems.
- Currently there are no tool, procedure, policy or agreement regarding cross provider forensic investigations.

- **Challenges regarding SLA:**
- Important terms regarding forensic investigations are not included in the SLA at the moment.
- This is because there is a lack of customer awareness, a lack of CSP transparency and a lack of international regulations.
- Most cloud customers are still not aware of the potential issues that might rise regarding forensic investigations in the Cloud and their significance.
- The consequence is that they might end up not knowing anything at all about what has happened in the Cloud in cases when their data is lost in criminal activities and has no right to claim any compensation.
- CSPs are not willing to ensure transparency to the customers regarding forensic investigations because they either do not know how to investigate cloud crimes themselves or the methods and techniques they are using are likely to be problematic in the highly complex and dynamic multi-jurisdiction and multi-tenancy cloud environment.
- The progress of any law and regulations including law and regulations of cyber crimes is very slow, while cloud computing is rapidly emerging as a new battlefield of cyber crimes for hackers who are equipped by the most updated techniques, investigators, law enforcement and various cloud organizations.

Challenges regarding Multi-Jurisdiction and multi-tenancy

- The legal challenges of multi-jurisdiction and multi-tenancy concern the differences among legislations in all the countries (states) the Cloud and its customers reside in.
- The differences between jurisdictions affects on issues such as what kind of data can be accessed and retrieved in the jurisdiction(s) where the physical machine(s) from which data is accessed and retrieved, how to conduct evidence retrieval without breaching privacy or privilege rights of tenants according to the privacy policies and regulations in the organizations and specific jurisdiction where multiple tenants' data is located, what kind of evidence is admissible to the court in the specific jurisdiction, what kind of chain of custody is needed in the evidence preservation in the jurisdiction(s) where forensic data has passed during an investigation in the Cloud.
- Multi-jurisdiction issues also concern lack of legislative mechanism that facilitates collaboration between industry and law enforcement around the world, in cases such as resource seizure, cloud confiscation, evidence retrieval, data exchange between countries, etc.

Opportunities

Cost Effectiveness

- Everything is less expensive when implemented on a larger scale, including security and forensic services.
- Cloud computing is currently very attractive to SMEs (Small and Medium Enterprises) due to the cost advantage which also applies to forensic implementations.
- SMEs that cannot afford dedicated internal or external forensics implementations or services may have an upgrade at relatively low cost when adopting cloud computing.

Data Abundance

- Amazon S3 and Amazon Simple DB ensure object durability by storing objects multiple times across multiple Availability Zones on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot to reduce the risk of single point of failure
- Data abundance generated in the Cloud is helpful to investigations as full data deletion cannot be guaranteed and investigators can take advantage of it to recover data as evidence.
- Scaled up to the Cloud, when a request to delete a cloud resource is made it actually technically can never result in true wiping of the data. Full data deletion may only be guaranteed by destroying the resource that is shared with other cloud tenants.
- Thus pieces or segments of data that is crucial to investigation are very likely to remain somewhere in the Cloud for the investigators to discover.

Overall Robustness

- cloud technologies help to improve the overall robustness of forensics in the Cloud.
- For example, Amazon S3 generates an MD5 hash automatically when you store an object. So theoretically, the cloud customers do not need to look for external tools to generate time consuming MD5 checksums.
- IaaS offerings support on-demand cloning of virtual machines. As a result, in the event of a suspected security breach, the customer can take an image of a live virtual machine for offline forensic analysis, leading to less downtime for analysis.
- Multiple clones can also be created and analysis activities parallelized to reduce investigation time. This improves the analysis of security incidents and increases the probability of tracking attackers and patching weaknesses.
- Amazon S3 allows customer to use “Versioning” to preserve, retrieve, and restore every version of every object stored in the S3 bucket.
- An Amazon S3 bucket can be configured to log access to the bucket and objects within it. The access log contains details about each access request including request type, the request resource, the requestor’s IP, and the time and date of the request (Amazon, 2010).
- All of these can be used to investigate abnormal incidents and application failures.

Scalability and Flexibility

- Cloud computing allows scalable and flexible usage of resources which also applies to forensic services.
- For example, it can provide unlimited pay-per-use storage of logs, allowing more comprehensive logging without compromising performance.
- Increase the efficiency of indexing, searching and various queries of the logs.
- Cloud instances can be scaled as needed based on the logging load.
- Forensic activities only take place when incidents happen which can largely take advantage of the cost-effectiveness of cloud computing.
- Customers have the choice to build their own dedicated forensic server in the Cloud, ready to use only in need.

Standards and Policies

- Cloud computing is a transformative technology which is changing the way IT is managed and generating a new wave of innovations.
- Cloud computing is still at its early stage and this is a unique opportunity to lay a standards and policies for cloud forensics that will evolve together with the technology until it matures.

Forensics-as-a-Service

- The concept of “Security as a Service” is emerging in cloud computing.
- For example, research has shown the advantages of a cloud platform for large-scale forensic computing and cloud-based anti-virus software.
- The emerging delivery models include established information security vendors changing their delivery methods to include services delivered through the Cloud, and start-up information security companies play as pure CSPs and provide security only as a cloud service and do not provide traditional client/server security products for networks, hosts, and/or applications.
- “Forensics as a [Cloud] Service” can be developed in the same way to make use of the massive computing power to facilitate cyber criminal investigations on all levels.

Impact of cloud computing on Digital Forensic

- "Cloud computing makes forensic harder", comments from participants can be concluded into following issues
  - Reduced access to remote and distributed physical infrastructure and storage
  - Lack of physical control and physical location of data
  - Lack of standard interface
  - Legal issues, including multiple ownership, multiple jurisdictions and multiple tenancies
  - Lack of collaboration from the cloud provider
  - Evidence segregation
  - Data recovery

- “Cloud computing makes forensic easier”, comments from participants can be concluded into following aspects
  - Cloud investigations can leverage characteristics of cloud computing.
  - Cloud investigations will be highly dependent on provider providing digital evidence through centralized administration and management, so there will be less work for investigator/law enforcement side.
  - Evidences in cloud environment are harder to destroy by criminals as they may be mirrored to multiple locations.
  - Investigative functionality can be integrated in cloud implementation.