류정현

17.09.24

DIGITAL FORENSICS

FORENSICS FRAMEWORK FOR CLOUD COMPUTING

OUTLINE

- Abstract
- Introduction
- Challenges in cloud forensics
- Proposed solution
- Conclusion
- Opinion

ABSTRACT

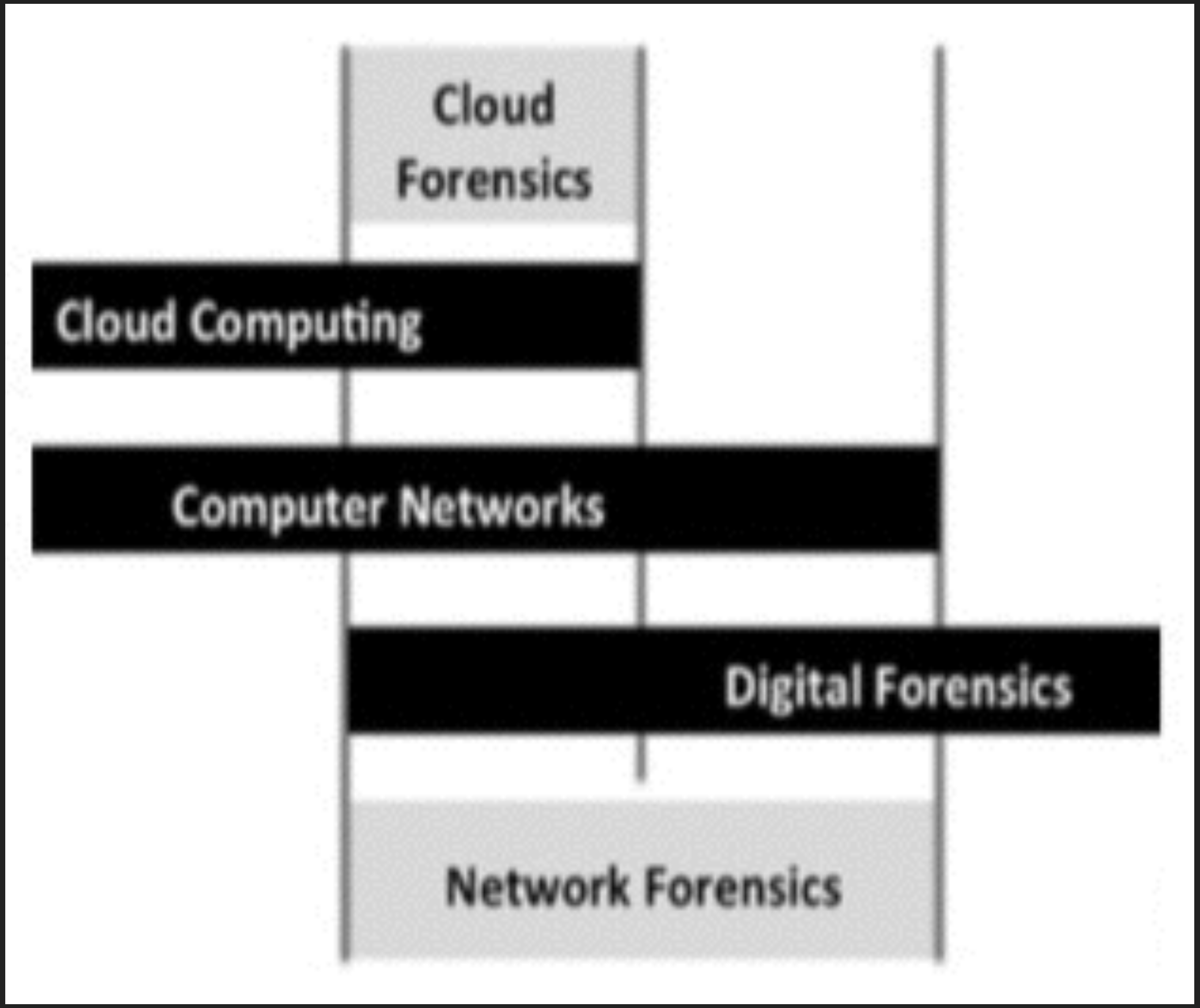
- The popularity of cloud computing has been on the rise in recent years.
- A recent survey reports success of the cyber criminals in using cloud computing technology.
- While mitigating cloud crime, investigators face several challenges and issues dealing with cloud forensics.
- In this paper, the challenges faced by forensic investigators are highlighted.
- The dependence on CSP includes the collection of data for the forensics process and there may be a chance of altering data that affects the entire investigation process.
- For mitigating the dependency on CSP, a new model for collecting forensic evidence outside the cloud environment is developed.

INTRODUCTION – CLOUD FORENSICS (1)

- "Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events. This is done through identification, collection, preservation, examination, and interpretation and reporting of digital evidence" - NIST
- "the application of digital forensic science in cloud environments as a subset of network forensics"
  - Ruan et al.

INTRODUCTION – CLOUD FORENSICS (2)

- 3 Different aspects
  - Technical : Tools, Mechanisms, Procedures
  - Organizational : Interaction between Cloud actors
  - Legal : Multi-jurisdictional, Multi-tenancy



INTRODUCTION - CLOUD COMPUTING

- "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" - NIST
- 3 Service models
  - Saas(Software as a service)
  - Paas(Platform as a service)
  - Iaas(Infrastructure as a service)

INTRODUCTION - DIGITAL FORENSICS

- An applied science to identify an incident, collection, examination, and analysis of evidence data.
- The phases of digital forensics :
  - Identification
  - Collection
  - Organization
  - Presentation

CHALLENGES IN CLOUD FORENSICS - DATA ACQUISITION

- This is the fundamental and vital step in the forensic procedure.
- Any flaw in this phase is passed on to the successive phases, resulting in transformation of the course of the investigation process.
- In cloud forensics, grabbing the equipment is infeasible owing to the multi-tenancy and remote nature of cloud computing.

CHALLENGES IN CLOUD FORENSICS - DATA ACQUISITION

- Some of the challenges faced by the investigators towards data acquisition in a cloud environment are as follows.
  - Physical inaccessibility
  - Less control in cloud
  - Volatile data
  - Trust issue
  - Multi-tenancy

PHYSICAL INACCESSIBILITY

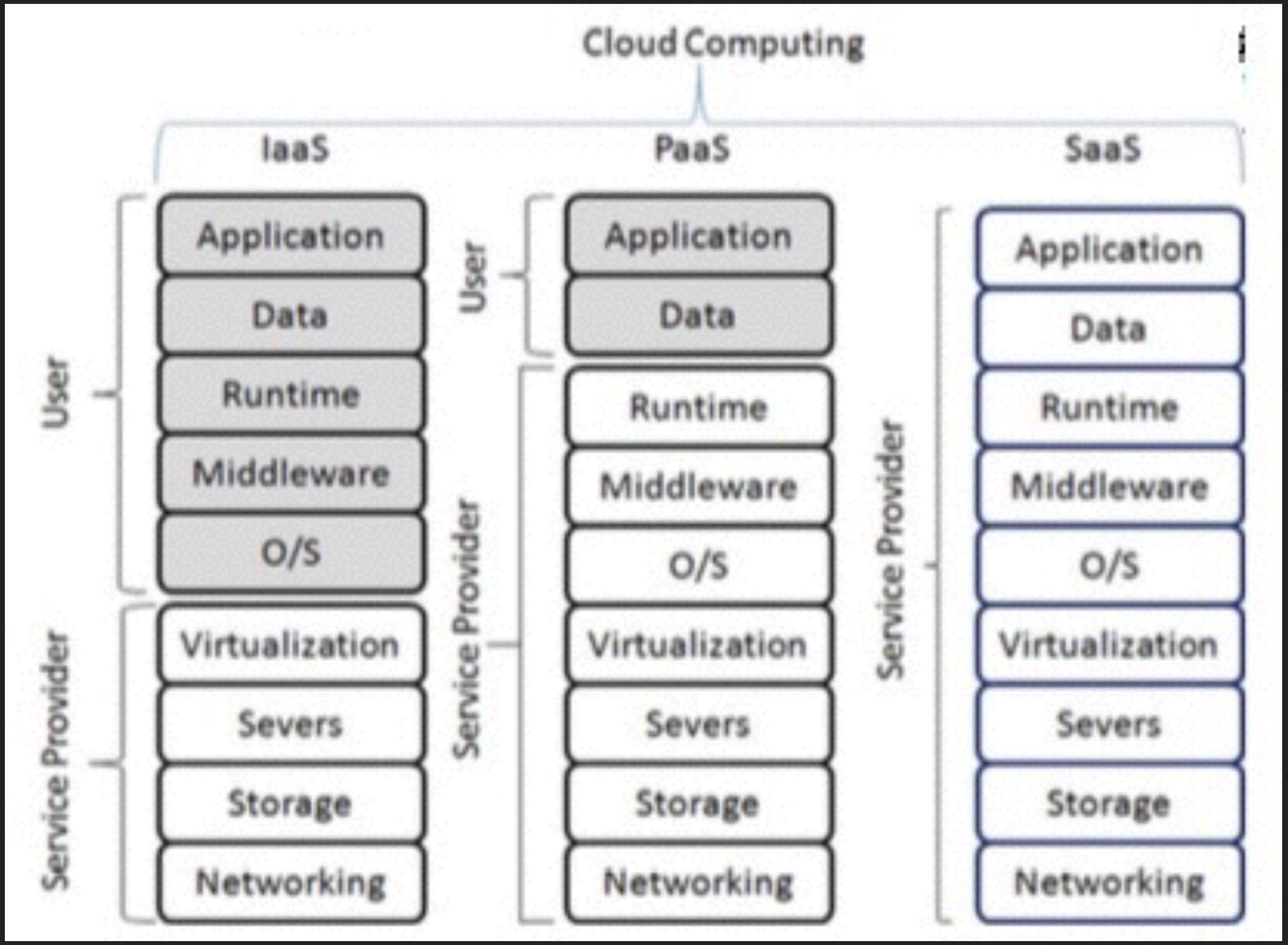
- Evidences are scattered and saved in different locations due to the significant characteristics of cloud. This leads to inaccessibility towards the collection of data and affects the data acquisition process.

LESS CONTROL IN CLOUD (2)

- In cloud, both users and investigators have restricted access, unlike digital forensics seizing of digital equipment is uncertain in the cloud.
- Even though access control is available for various levels in the cloud, forensics investigators have to anticipate Cloud Service Provider (CSP) for collecting data.
- A cloud server cannot be seized by the investigator despite reaching the location due to its multi-tenant nature.

LESS CONTROL IN CLOUD (1)

- Only logs related to the application can be accessed by the investigator in the SaaS and PaaS models.



- Access control to each model

VOLATILE DATA

- Virtual Machines (VM) are used by service providers for provisioning their customers.
- In this VM, volatile data like registry entries or temporary internet files will be lost if it is not synchronized with storage devices like Amazon S3, all information in VM is erased when VM gets restarted or shutdown.

TRUST ISSUE

- The investigator needs an internal staff to assist him in collecting data.
- Sometimes this person may be from the same CSP or may not be a certified investigator and this may affect the integrity of data to be produced in law.

MULTI-TENANCY

- In cloud computing, different clients share individual resources.
- While acquiring evidence from cloud, two issues are addressed by the investigator.
- To start with, he has to prove that the extracted data is not mingled with other's data and has to maintain the integrity of the other user's data.

CHALLENGES IN CLOUD FORENSICS - LOGGING

- The logs may be process logs, application logs, system logs or network logs. These are the key for the investigation process, but getting this log data from the cloud is a crucial one. Several challenges that are recognized while obtaining logs are as follows.
  - Decentralization
  - The volatility of logs
  - Accessibility of logs

DECENTRALIZATION

- In cloud, the logs are spread all over the network. Due to this phenomenon, the gathering of logs from various sources becomes difficult for cloud investigators.

THE VOLATILITY OF LOGS

- Virtual Machines are used by CSPs for providing service to their customers. In the case of VMs, the volatile data like temporary internet files, registry data is completely lost once VM gets restarted or shutdown.

ACCESSIBILITY OF LOGS

- There is no procedure or method for accessing logs in distinct places and the logs are used for troubleshooting, debugging, etc.

CHALLENGES IN CLOUD FORENSICS - DEPENDENCE ON CSP

- Logs are collected and stored at CSP premises requiring the need for the investigators and the users to depend on CSPs for accessing network logs and server logs. In this point, CSP may tamper logs.

CHALLENGES IN CLOUD FORENSICS - CHAIN OF CUSTODY

- The chronology of the ownership, custody or location of a historical object, document or group of documents.
- In the case of cloud forensics, this is not applicable because of its multi-jurisdictional laws and procedures.
- The investigators have to depend on CSP for acquiring the chain of custody.

CHALLENGES IN CLOUD FORENSICS - CRIME SCENE RECONSTRUCTION

- Crime scene reconstruction is infeasible in a cloud environment as data in VM gets erased completely when VM gets power off or rebooted.

CHALLENGES IN CLOUD FORENSICS - CROSS BORDER LAW

- Data centers afforded by cloud providers are distributed worldwide, so the cross-border law is an important issue in cloud forensics.
- The investigation process should be carried under the laws in the specific jury, whereas the measures for preserving data and chain of custody differ according to the jury and the entire investigation process will be affected by the cross-border law.

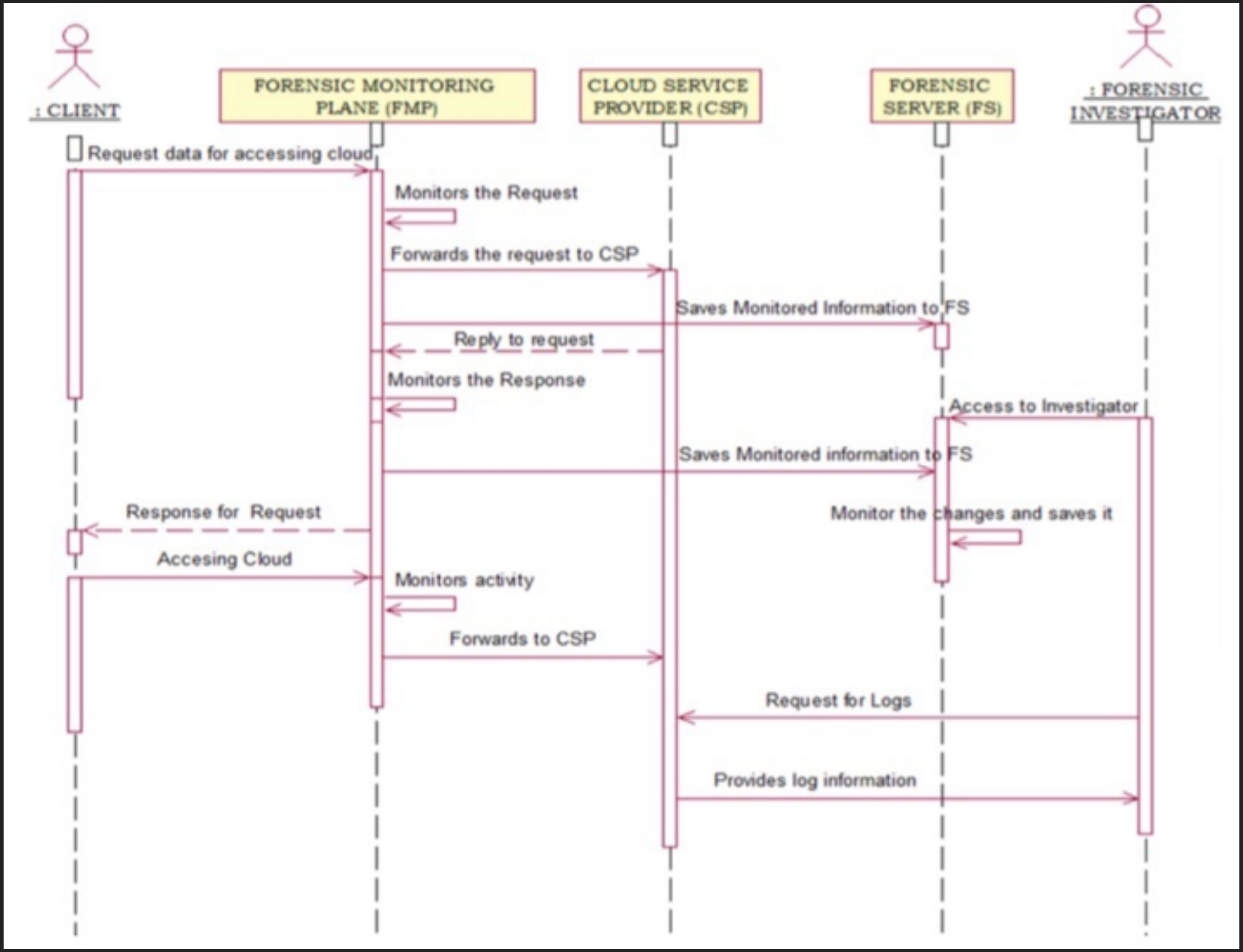
CHALLENGES IN CLOUD FORENSICS - LAW PRESENTATION

- Presentation under jury is the final step in both digital and cloud forensics.
- In a cloud environment, thousands of VMs run in cloud data centers and hundreds of users are accessing simultaneously.
- This creates a serious challenge in cloud forensics than digital forensics.

PROPOSED SOLUTION

- The proposed solution addresses the data collection issues discussed in literature by introducing a centralized forensic server and a forensic layer called forensic monitoring plane (FMP) outside the cloud Infrastructure, after obtaining permission from the international telecommunication union (ITU).

PROPOSED SOLUTION



PROPOSED SOLUTION

- The client initiates the request to the cloud service provider.
- The request and response are intercepted by FMP monitoring tool which forwards the request to the server and the response to the client, and at the same time, it forensically images the request and saves it in the forensic server.
- Forensic investigator logs into the forensic server for analyzing the evidence collected.
- Actions in the forensic server also get forensically imaged and saved in the forensic server. If the investigator suspects the CSP, he initiates the request for evidence sources from CSP and compares with one another, and hence the integrity of the collected data also gets verified.

CONCLUSION

- The need for cloud forensics is on the rise, because of its rapid growth in cloud computing and due to the possibility of cloud-related crime occurring in the digital world.
- There are many challenges in cloud forensics and only a few researchers have addressed these challenges.
- In this paper, the challenges faced in cloud forensics and corresponding solutions addressed by the researchers have been highlighted in depth.

OPINION

- It makes sure that various malicious activities should be detected.
- This framework should never degrade the performance of cloud services.
- It should be able to satisfy both accessibility and reliability.

THANK YOU.