ENABLING FORENSICS-AS-A-SERVICE FOR CLOUD COMPUTING SYSTEMS

Sumaiya Safoorah[1], Dr. Syeda Asra[2]

[1]PG Student, Department of Computer Network, Sharnbasva University, Karnataka, India
[2] Professor, Department of Computer Science, Sharnbasva University, Karnataka, India

---***---

Abstract - *Ongoing assaults on the cloud condition features the need for leading scientific examinations. In any case, performing legal sciences in the cloud is not the same as customary condition. Adjusting the equivalent, National Institute of Standards and Technology (NIST) recorded in excess of 65 difficulties for cloud legal sciences. Despite the fact that cloud is a XaaS supplier, Forensics-as-a-Service was excluded from that rundown. There are different specialized, authoritative and lawful explanations behind it. In any case, performing examination in the cloud condition is basically conceivable just if uphold from the Cloud Service Provider (CSP) is made accessible. Our proposed model-FaaSeC can expand the legal help from CSP and make CSP to give Forensics-as-a-Service (FaaS) to the specialist.*

Key Words: **Cloud Computing, Digital Forensics, Log analysis, Event Reconstruction**

1. INTRODUCTION

The development of cloud market has reached past the normal. It advantages the end clients by offering continuous types of assistance at lesser expense and with decreased support overheads. Be that as it may, the ongoing assaults announced in the cloud bring up a few issues on its security. These security breaks caused trust shortage in the cloud. Two potential arrangements exist in this unique circumstance. One is to improve the security of the current calculations and the subsequent arrangement is to perform scientific examination in the cloud. In this paper, our advantage is on the last mentioned.

We found that till date, there is no merchant which encourages the legal examination in the cloud condition. There are different legitimate and specialized explanations for cloud suppliers reluctance to give FaaS to the outsider faculty. The fundamental driver is its multi-occupant nature as the outsider agent may get an opportunity to obtain different inhabitants information during criminological examination. This prompts protection infringement of the relating clients and is treated as an offense. Our answer considers the above issue and expands the opportunity of encouraging FaaS to the outsider staff by the CSP. The focal points in utilizing FaaS models for the cloud condition are.

The scientific cycle in researching the relics of cloud environment can be known. (ii) When FaaS models are coordinated with the pertinent legal apparatuses, it prompts legitimately permissible legal examination. (iii) It can help in giving far reaching cloud scientific answers for make a repeatable framework. (iv)It can be utilized to upgrade the understanding about the procured cloud relics . The outsider specialist might be trusted or untrusted. In this paper, we handle the most dire outcome imaginable for example at the point when the specialist isn't trusted and offered admittance to the cloud framework, there are high possibilities that he/she may perform dubious exercises. The untrusted examiner might be inside to the cloud association as a component of episode people on call group or can be an outside substance. When he/she is offered admittance to the cloud foundation, there are high odds of proof altering. This surely prompts create a legal report with misdirecting ends. Along these lines, we recommend that CSP encouraging FaaS should know the occasions/exercises being performed by the examiner at the cloud end. This can improve the CSP ability to encourage legal administrations to the agent. Accepting this as base, we propose a model to be specific, FaaSeC which can distinguish the dubious exercises performed by the untrusted examiner in the cloud.

1.1 Problem statement

Since the specialist is given the entrance for the cloud framework during the legal cycle, he/she can abuse the chance to play out any dubious movement.

1.2 Objective of the system

We planned an extensive measurable cycle with the end goal that (I) the odds of CSP offering legal types of assistance to the agent would expand (ii) The straightforwardness in the cloud scientific cycle is improved by making legal logs at the cloud end. (iii) We propose two methodologies specifically SeMS and CoPS which can mechanize the location of dubious occasions/measures from criminological logs at the cloud end.

2. SYSTEM ANALYSIS

2.1 Existing System

For performing conventional advanced criminology, the specialist may follow different stages Identification, Preservation, Collection, Examination, Analysis and Presentation. The cycle engaged with each stage can't be straightforwardly applied to the cloud condition due to the multi-tenure, absence of straightforwardness and fast flexibility properties of cloud.

(1)The specialist can be reliable and utilizes CFT for playing out all the solid exercises. (2) The examiner can be untrusted and performs dubious exercises utilizing CFT. Here, a movement can be delegated solid/dubious dependent on the entrance control arrangements given to the agent. On the off chance that he/she abuses those arrangements then it comes in the classification of dubious else it is treated as solid action. For instance, if the specialist got to the information of an occupant for which he/she doesn't have consents then it falls in to the classification of dubious. Since the agent is given the entrance for the cloud foundation during the scientific cycle, he/she can abuse the chance to play out any dubious action.

DISADVANTAGES:

- Since the examiner is given the entrance for the cloud foundation during the measurable cycle, he/she can abuse the chance to play out any dubious action.

2.2 Proposed System

We planned an exhaustive criminological cycle with the end goal that the odds of CSP offering legal types of assistance to the examiner would expand (ii)The straightforwardness in the cloud measurable cycle is improved by making scientific logs at the cloud end. (iii) We propose two methodologies specifically SeMS and CoPS which can computerize the recognition of dubious occasions/measures from criminological logs at the cloud end. Utilizing SEMS and Cops we can discover dubious arrangements from cloud measurable application.

ADVANTAGES:

- SeMS and CoPS are planned so that, they can be applied to identify dubious arrangements in any application log.
- FaaSeC Model gives the total cycle of offering legal as a support beginning from the agent enlistment to report age.
- The dubious occasions from the CFI log were distinguished consequently absent a lot of human exertion.

3. METHODOLOGY

In this project work, I have used four modules and each module has own functions, such as:

- Data User module
- Investigator Module
- CSP
- COPS and SEMS Module

3.1 Data User module

In the first module, we develop the Data User Module. Owner Will Sign up and upload data to cloud server with private key and encryption. After Getting key Owner can authenticate data using key, and upload any data related to users to cloud. In this module, data owner will check the progress status of the file upload by him/her. It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of viewing his own data and executing **Encrypt and key generation** operation. After the completion, owner logout the session

3.2 CSP module

We develop cloud service provider module which will handle authentication and verification of investigator. CSP can view all uploads of different users. CSP can't view user data as it is in encrypted state. He don't have permission to view user data.

CSP will view investigator log files with time and owner name. Taking this data as input for both algorithms (sems and cops) CSP will analyze which investigator is attacker. Based on the output of algorithms he will finalize attackers and normal investigator and unauthorized attackers.

3.3 Investigator module

We develop Investigator Module. Investigator will register with application and request for registration is sent to CSP for verification. After CSP accepts investigator request then only he can login in to application.

Investigator can view data of any owner which are uploaded by respective owner but he can't view data directly without verification from data owner.

Investigator will send data view request to data owner who will respond to request and authenticate by sending key which is used to decrypt data.

3.4 COPS and SEMS module

We use TKS to initially get the top-k frequent item sequences. Then SEMS is applied to get the suspicious sequences.

Say, the CSP is interested to know the suspicious sequences in CFI log,then each new sequence in the log during Time Window T is compared with the frequent item sequences (freqseq). If a mismatch occurs, the percentage of fraction left (*per fractionLeft*) will increase and if it is more than the user threshold (*thseq*) value then it is considered as suspicious sequence. We can also get the suspicious sequences of a cloud forensic application using conditional probability. In COPS we use two method for conditional probability.

1. Threshold value checks
2.Key mismanagement

4. SYSTEM ARCHITECTURE:

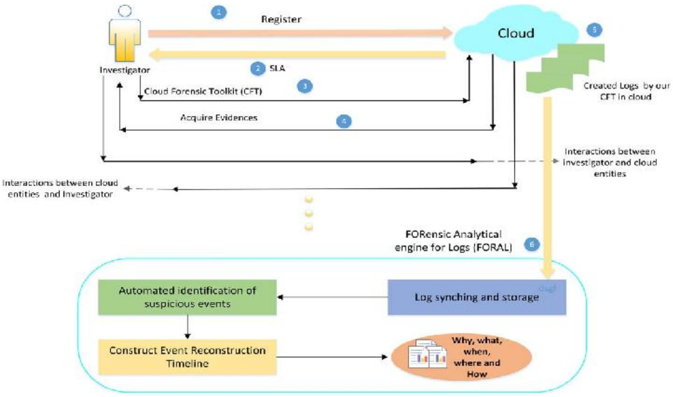

1
Register
Cloud
5
Investigator
2 SLA
Cloud Forensic Toolkit (CFT)
3
Created Logs by our CFT in cloud
Acquire Evidences
4
Interactions between investigator and cloud entities
Interactions between cloud entities and Investigator
FORensic Analytical engine for Logs (FORAL)
6
Automated identification of suspicious events
Log synching and storage
Construct Event Reconstruction Timeline
Why, what, when, where and How

Fig. 4: system architecture

System architecture is as shown above. Where Investigator needs to register to the cloud to access the user uploaded file. First Investigator sends a request to the cloud. CSP needs to give authority to the investigator for accessing files.. After getting access from CSP, Investigator sends a request to the user to access the file. User sends a response to the Investigator by sending a secret key to the email id of investigator. Investigator uses secret key to access the file of user. Investigator can trusted or untrusted. In some cases when The Investigator is untrusted then it can harm the user file by misusing it. CSP uses two techniques that is SeMs and CoPs to check whether the Investigator is attacker or not.

5. RESULT AND DISCUSSION

Below snapshot shows the home page of enabling forensics as a service for cloud computing system

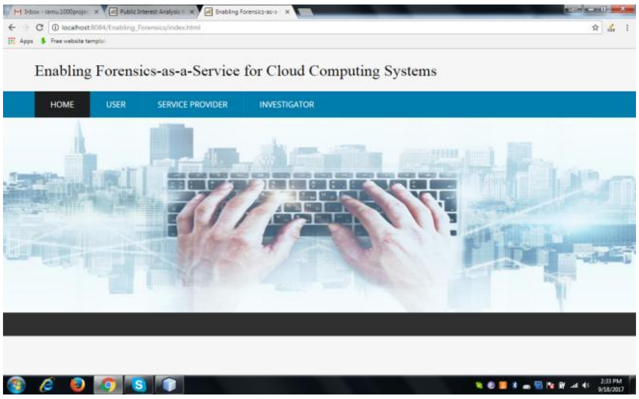


Fig. 5.1: Home Page

For uploading file user needs to register , below snapshot shows the user registration page.

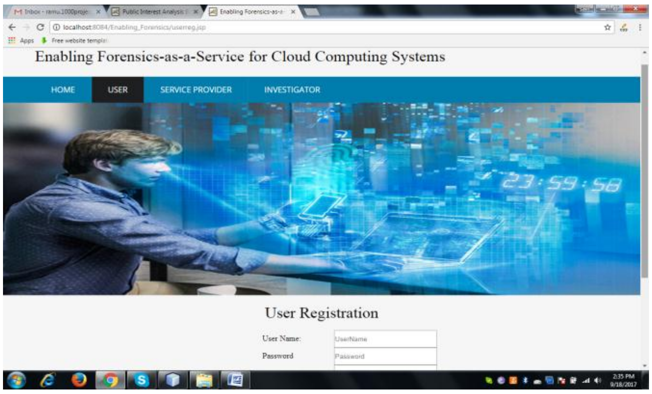


Fig. 5.2: User Registration

After registration user needs to login , below snapshot shows the user home page. User needs to upload a file to send a request and user can also view files from the user home page. Below snapshot shows the upload file page.

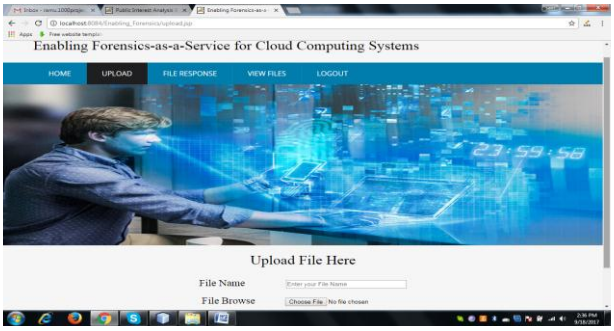


Fig. 5.3: File Upload Page

After uploading a file, the file data will be in decrypted form as shown in below snapshot.

Investigator needs to register to access the uploaded files, below snapshot shows the registration page of Investigator. Afterregistration,Investigatorneedstologin, after investigator login below snapshot shows the home page of investigator.

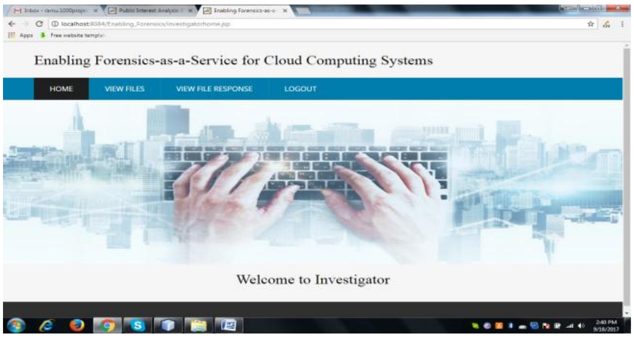
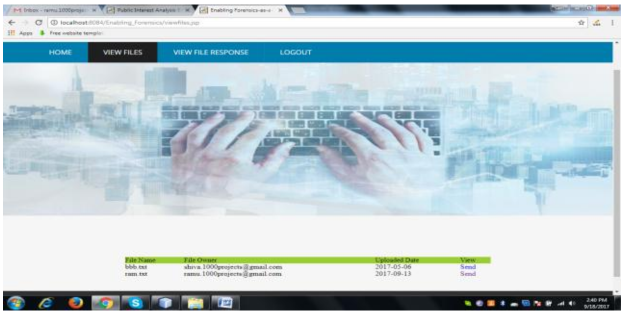


Fig. 5.4: Investigator home page

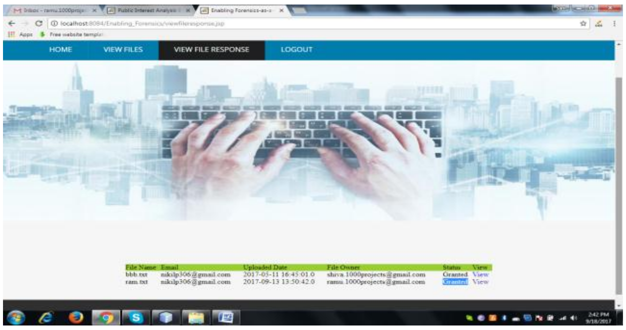
When an investigator needs to access a file, it should send a request



File Name	File Owner	Uploaded Date	View
bbb.txt	shiva.1000projects@gmail.com	2017-05-06	Send
ram.txt	ramu.1000projects@gmail.com	2017-09-13	Send

Fig. 5.5: View File and Send Request

User send a response to the investigator that is it permits investigator to access the file.



File Name	Email	Uploaded Date	File Owner	Status	View
bbb.txt	nikilp306@gmail.com	2017-05-11 16:45:01.0	shiva.1000projects@gmail.com	Granted	View
ram.txt	nikilp306@gmail.com	2017-09-13 13:50:42.0	ramu.1000projects@gmail.com	Granted	View

Fig. 5.6: View File Response From User

Service provider is the one who provides service to the user and investigator.

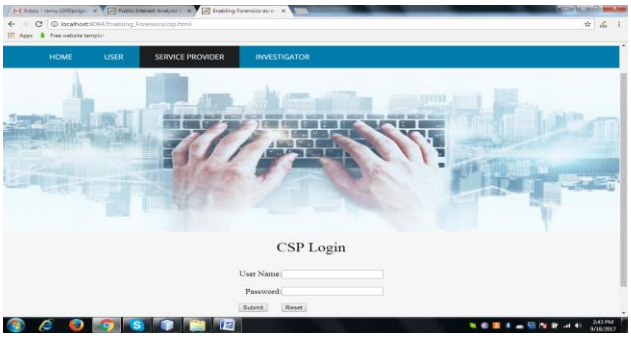


Fig. 5.7: CSP login page

This is the home page of service provider, CSP needs to provide authority to the investigator. The Upload page shows all the files uploaded by user.

SeMS is the technique applied to know whether the investigator is attacker or not. Investigator is attacker when it views data for more than 2minutes.

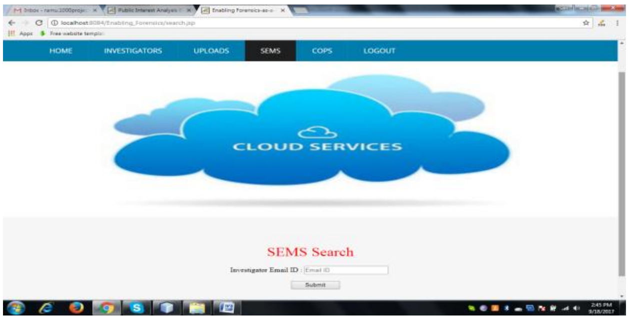


Fig. 5.8: SEMS Search

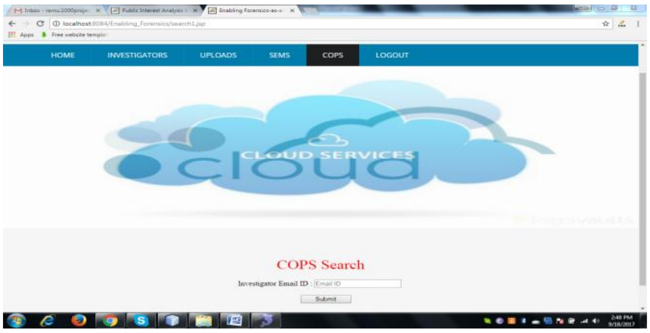


Fig. 5.9: COPS Search

6. CONCLUSION

Late assaults in the cloud frameworks show the significance of performing criminological examination in such situations. Crime scene investigation in the cloud condition is at an early stage and requires the cloud supplier uphold for encouraging FaaS. We proposed another Cloud Forensic Service model called FaaSeC. This model makes the legal application sign in the cloud from which the CSP can realize the exercises performed by the outsider specialist. For criminological examination, distinguishing the dubious occasions assumes a critical job and we discover those occasions from the cloud measurable application log utilizing SeMS and CoPS. We additionally looked at both the methodologies regarding execution time and memory utilization.

7. REFERENCES

[1] Sutte J.: Twitter hack raises questions about cloud computing,
In:
http://edition.cnn.com/2009/TECH/07/16/twitter.hack/, (2009), accessed 21-07-2013.

[2] Higgins K.: Dropbox, wordpress used as cloud cover in newapt attacks,
In:http://www.darkreading.com/attacksbreaches/dropbox-wordpress-used-as-cloud-coverin/240158057, (2013), accessed 22-07-2013.

[3] Inci, Mehmet Sinan, et al,: Seriously, get off my cloud!Cross-VM RSA Key Recovery in a Public Cloud. In: IACR Cryptology ePrint Archive, 2015.

[4] Kumar, Puneet, and Harwant Singh Arri. Data location in cloud computing. International Journal for Science and Emerging Technologies with Latest Trends 5.1 (2013): 24-27.