ISSN: 2456 - 4664
International Journal of Advanced Trends in Engineering and Technology
Impact Factor 5.965, Special Issue, April - 2018
International Conference on Innovations & Discoveries in Science, Engineering and Management
On 9th & 10th April 2018 Organized By
Vaageswari College of Engineering, Karimnagar, Telangana

WORKFLOW MANAGEMENT AND PROCESSING USING CLOUD

V. Bhavana*, P. Radhika & Dr. Y. Jahnavi*****
* UG Student, Department of CSE, Geethanjali Institute of Science and Technology, Kovur, Nellore, Andhra Pradesh
** Associate Professor, Department of CSE, Geethanjali Institute of Science and Technology, Kovur, Nellore, Andhra Pradesh
*** Professor, Department of CSE, Geethanjali Institute of Science and Technology, Kovur, Nellore, Andhra Pradesh

Cite This Article: V. Bhavana, P. Radhika & Dr. Y. Jahnavi, "Workflow Management and Processing Using Cloud", International Journal of Advanced Trends in Engineering and Technology, Special Issue, April, Page Number 4-6, 2018

Abstract:
Late assaults on the cloud condition features the need for directing scientific examinations. Be that as it may, performing legal sciences in the cloud is unique in relation to customary condition. Acclimating the same, National Institute of Standards furthermore, Technology (NIST) recorded in excess of 65 challenges for cloud legal sciences. Despite the fact that cloud is a XaaS supplier, Legal sciences as-a-Service was excluded in that rundown. There are different specialized, hierarchical and legitimate purposes behind it. In any case, performing examination in the cloud condition is for all intents and purposes conceivable just if bolster from the Cloud Service Supplier (CSP) is made accessible. Our proposed demonstrate FaaSeC can broaden the measurable help from CSP and make CSP to give Forensics-as-a-Service (FaaS) to the examiner.

Key Words: Distributed Computing, Digital Forensics, Log Investigation & Event Recreation

1. Introduction:

The developments of cloud advertise has come to past the normal. It benefits the end clients by giving continuous administrationsat lesser cost and with diminished support overheads. In this paper, we handle the most dire outcome imaginable i.e. at the point when the examiner isn't trusted and offered access to the cloud foundation; there are high shots that he/she may perform suspicious exercises. The untrusted examiner might be inner to the cloud association as a major aspect of occurrence specialists on call group or can be an outside substance. When he/she is offered access to the cloud framework, there are high odds o proof altering. This in reality leads to create a scientific report with misdirecting conclusions. In this way, we recommend that CSP encouraging FaaS should know the occasions/exercises being performed by the specialist at the cloud end. This can enhance the CSP ability to encourage criminological administrations to the agent. Taking this as base, we propose a model in particular, FaaSeC which can identify the suspicious exercises performed by the untrusted examiner in the cloud.

Commitments of the Paper: (I) We planned a far reaching legal process with the end goal that the odds of CSP giving scientific administrations to the agent would expand (ii) The straightforwardness in the cloud measurable process is enhanced by making criminological logs at the cloud end. (iii) We propose two approaches in particular SEMS and COPS which can mechanize the identification of suspicious occasions/forms from legal logs at the cloud end.

Association of the Paper: The proposed demonstrate FaaSeC (Forensic-as-a-Service for cloud frameworks) is portrayed. The procedure behind the two methodologies (SEMS and COPS) to distinguish forensically intrigued occasions from the criminological logs is talked about. Both the methodologies are approved utilizing a run of the mill investigative situation

2. Related Work:

Our model begins encouraging FaaS promptly after the outsider specialist registers with the cloud provider. The enrollment process ought to be standard and lawfully acceptable. The enlistment will be evaluated by the cloud elements and after that in like manner SLAs are set up upon common trust. From that point, the specialist can begin the procedure of criminology utilizing any cloud measurable toolbox (CFT). We utilized CFI apparatus (Cloud Forensic Investigator) for testing the proposed FaaSeC demonstrate. We utilize CFI and CFT reciprocally. CFI is our created device and it is utilized to perform measurable examination in IaaS cloud [14]. Now, there are two potential outcomes: (1) The specialist can be dependable and utilizes CFT for playing out all the solid exercises. (2) The specialist can be untrusted what's more, performs suspicious exercises utilizing CFT. Here, a movement can be delegated solid/suspicious in view of the get to control arrangements given to the specialist. On the off chance that he/she abuses those strategies then it comes in the classification of suspicious else it is deal with as solid action. For instance, on the off chance that the specialist got to the information of an inhabitant for which he/she doesn't have authorizations then it falls in to the classification of suspicious. Since the examiner is given the entrance for the cloud framework amid the criminological procedure, he/she can misuse the chance to play out any suspicious action. The CSP ought to know about the exercises being performed by the agent when utilizing any CFT. We propose to accomplish this by making CFI log at the cloud side. This log is fundamentally an application log and contains the data like, the timestamp showing the specialist login time, areas being gotten to by the agent, indicating the items being read alongside the relating time, the rundown of relics procured by the specialist, the time taken to gain each ancient rarity, the IP from which the agent got to the cloud, the articles changed by the agent alongside its entrance and adjustment time, occasion showing the session shutting time and so on.

3. Procedure:

Putting the thought in straightforward terms, the CSP will be by and large unwilling to offer access to the cloud framework for the investigative reason. On the off chance that the cloud supplier knows each movement performed by the agent, at that point the CSP would co-work. We propose to accomplish this by legitimately logging every one of the exercises performed by CFI in cloud. By breaking down the CFI log, the CSP can know whether the exercises performed by the outsider specialist are suspicious or not. Continuously, examining cloud application logs is a tedious activity. We lessen this time with our Legal

ISSN: 2456 - 4664
International Journal of Advanced Trends in Engineering and Technology
Impact Factor 5.965, Special Issue, April - 2018
International Conference on Innovations & Discoveries in Science, Engineering and Management
On 9th & 10th April 2018 Organized By
Vaageswari College of Engineering, Karimnagar, Telangana

Analytical motor for Logs (FORAL). It contains different modules as appeared in Figure 1 and every one of them is informed beneath:

SEMS: We watched that, the kind of occasions which are available in the application logs are constrained. So we relegated a one of a kind number for every occasion and that pre-prepared log is appeared in Figure 2. Every extraordinary number speaks to an occasion produced by the agent utilizing CFI. For instance, nearness of occasion "1"in the pre-processed log shows that new case protest has been summoned, number "2" demonstrates that the subtle elements of the case are entered by the agent.

COPS: We spoke to the groupings in given Time window T utilizing trie information structure. At that point iterated through trie for each non-T grouping of the application and refreshed the check ofeach hub for the coordinating prefix. The likelihood of occasion event P in the grouping is figured utilizing Algorithm 2. In the event that the likelihood of any occasion is not as much as the given limit then we thought about that as suspicious. The correlation amongst SEMS and COPS is appeared in Table 1. Condensing it, execution time for SEMS is high than COPS and the memory utilization for COPS is high when contrasted and SEMS.

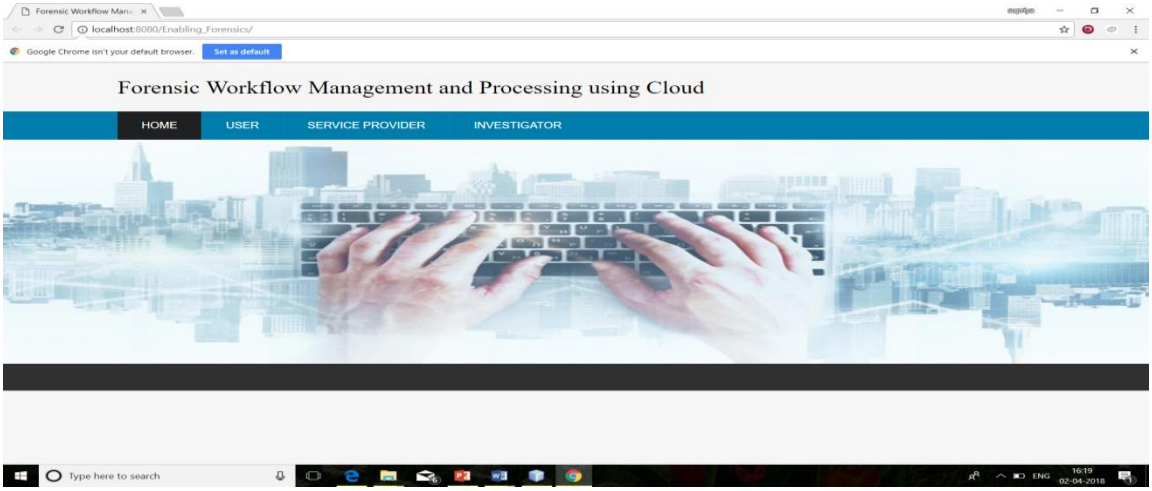
Since SEMS and COPS alarm the CSP at whatever point specialist plays out any suspicious action in cloud, the degree of CSP bolster for encouraging Forensics-as-an administration would increase.

Table 1: Comparison between SeMS and CoPS

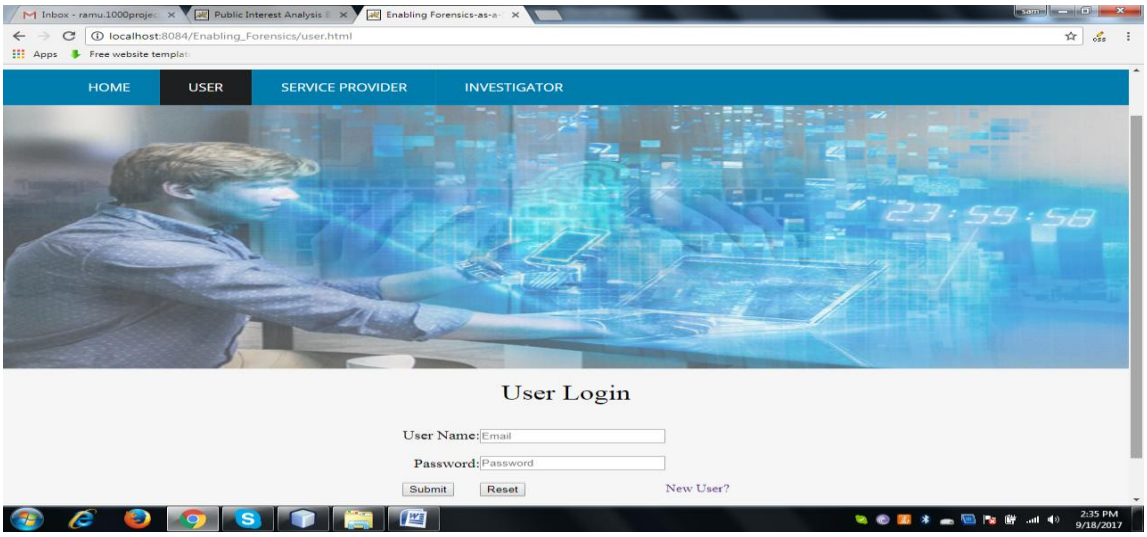
No. of sequences	Total Time (ms) for SeMS	Peak Memory (mb) for SeMS	Total Time(ms) for CoPS	Peak Memory (mb) for CoPS)
10	22	1.81805603	11	1.890281577
1450	130	6.30869293	91	7.572235107
4350	184	15.12903595	162	19.5663223
142100	709	79.12886047	519	81.42918396
2121600	7356	709.9880905	3797	711.2549823

4. Results:

Home:

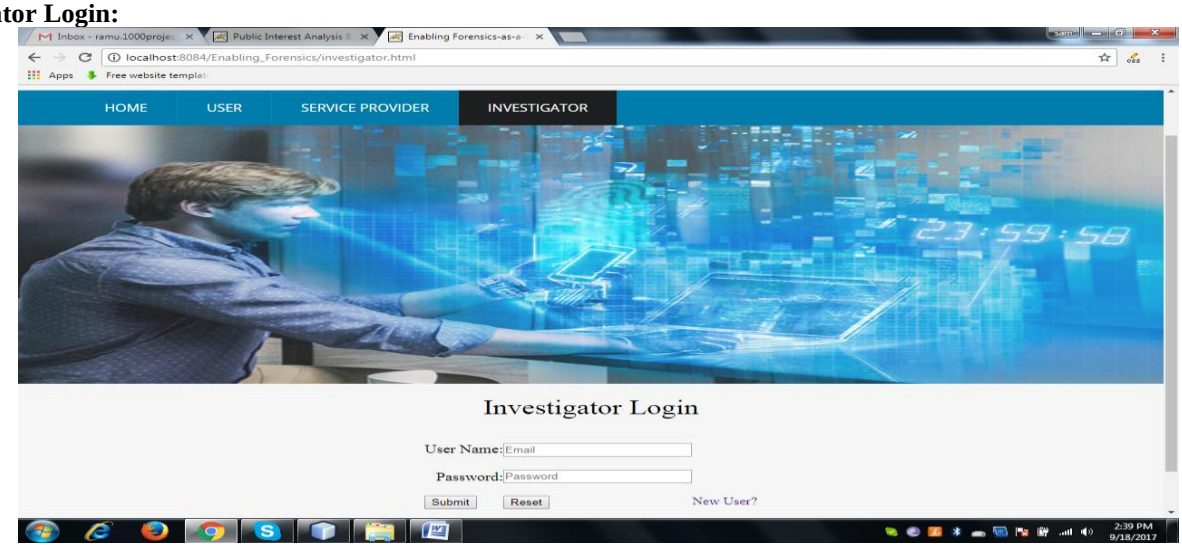


User Login:



ISSN: 2456 - 4664
International Journal of Advanced Trends in Engineering and Technology
Impact Factor 5.965, Special Issue, April - 2018
International Conference on Innovations & Discoveries in Science, Engineering and Management
On 9th & 10th April 2018 Organized By
Vaageswari College of Engineering, Karimnagar, Telangana

Investigator Login:



5. Conclusion:

Late assaults in the cloud frameworks demonstrate the significance of performing scientific examination in such situations. Crime scene investigation in the cloud condition is at an early stage and requires the cloud supplier bolster for encouraging FaaS. We proposed another Cloud Forensic Service show called FaaSeC. This model makes the measurable application sign in the cloud from which the CSP can know the exercises performed by the outsider specialist. For measurable investigation, recognizing the suspicious occasions assumes a critical part and we find those occasions from the cloud measurable application log utilizing SEMS and COPS. We likewise thought about both the methodologies in terms of execution time and memory Utilization.

6. References:

1. Akarsu B, Bayram K, Slisko J, Corona Cruz A. International Journal of Scientific Research and Education. Ijsae.in [Internet]. 2013; 6(3):221–32. Available from: http://ijsae.in/ijsaeems/index.php/ijsae/ article/viewFile/157/137
2. Birk D, Wegener C. Technical issues of forensic investigatinos in cloud computing environments. Syst Approaches to Digit Forensic Eng. 2011;
3. Dam M, Chen K. On the Security of Cloud Storage Services. MartindamDk [Internet]. 2011; Available from: http://martindam.dk/wp-content/uploads/cloudstorage.pdf
4. Foster I, Zhao Y, Raicu I, Lu S. Cloud Computing and Grid Computing 360-Degree Compared.