International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

# Review the Digital Forensic Techniques for Cloud Computing Environment

**Sonali Ogra[1], Prof. Praneet Khare[2]**

**Abstract:** ***Cloud computing services will develop a novel challenge for forensic investigators in conducting their analysis. Consequently, forensic investigators requirement to have systematic and current approach to accumulate forensic evidence that is allowable to the court. Even still computer forensic investigations connecting Cloud Computing systems are probable to necessitate additional time and determination to assume due to the quantity of computing devices inside the cloud, it still requirements to be forensically examined. The proposed forensic approach has been established to be applicable in IaaS cloud environment. Until today, there are still lack quantities of research connected to forensic approach in IaaS Cloud Computing situation which can be used in conducting forensic exploration. To proposed approach based on computation neural network for forensic investigators in cloud environment.***

**Keywords:** Cloud Computing, IaaS Cloud, Digital Forensic, Network Forensics Framework, virtualization

## 1. Introduction

Currently Internet is the pivot of our world, and the World Wide Web (WWW) is the key to Access it. To develop communication on internet networks and trust responsive documents to online services. Desktop application are occurrence return by completely periphery requests that can be approach in since numerous devices. This is probable appreciation to advanced web technologies that are being presented at enormously fast pace. However, these advance method at a price. Currently, the web is the foremost resources used by cyber-criminals to transmit out attacks nearby people and organization. In a condition where information is extremely dynamic and random, the fight against cyber-crime is suitable additional and added complicated [1]. this work is to stimulate research next to novel generation crimes. The primary part is added focused on a forensic point-of-view, and address a quantity of issue linked to the development of digital evidence. In demanding, it elucidate how the detonation of the network announcement replica has actual misused our association with technology and, as consequence, our behavioral patterns. In particular, to understanding the limitations of existing investigation technique when dealing with contemporary digital substantiation like online documents, data sending and getting and so on. We study how it is possible to leverage widespread Internet services in arrange to forge digital evidence, which can be oppressed by a cyber-criminal, in the condition of a testing, in control to claim a digital explanation. Additionally, a narrative technique to analyze cyber-criminal behavior on the Internet is proposed. This technique authorization obtain information from enormously dynamic resources, such as online social networks and clouding storage services, although conserve reliability, strength and volatility of the composed data.

These measures could be occupied after a crucial levels and in adding anomalous state as well. That might include dissimilar security actions that should be represented by cloud administration. Few of such measures. Malevolent User Detection: The events can be occupied to recognize whether the client who have login to the record is real or particular malignant client, who requirements to recover the information of particular other genuine clients. To complete this quantity cloud administration provider can request that the client produce additional perplexing and solid secret key at the season of creation his record. The administration supplier can exploit a multi-way security validation code check each time when customer login to his record. Our proposed CNN based approach could be set in a method that every time when the client login to his record, a validation inquiry can be requested whose response ought to organise with the genuine information secure in the cloud database.

Lately, few researches were focussed on defining a well-accepted models and methods for cloud digital forensics. Some are good and others are not so truthful. Additionally, particular studies did gather the stat of art of existing methodologies presented till currently of what is proposed. That's the reason why in this paper the foremost objective is not assembly the complete proposed research in this area, but we proposed to deliberate the greatest appropriate ones from an applicability point of view, and then contemporary our approach.

The rest of the paper is organized as follows. Section II throws some insight into the the literature are highlighted in Section III. Proposed methodology towards mitigating challenges are assumed in Section Conclusions V.

## 2. Related Work

This section highlights the existing solutions considered by researchers for qualifying specific challenges in cloud forensics.

Hraiz, S. et al[1]Presently, cloud computing is used mostly. As a consequence of that, novel challenges face the investigators in their work to extract the evidences. This paper highlights selected of these challenges and discussions the possible resolutions to mitigate or to solve these challenges. The tests were covered in this paper are gathering logs, volatile data, creation forensic image, and data integrity. The models of the cloud aren't affected in the similar technique with these challenges. The best model for the investigators is IaaS model, since the clients have control completed the infrastructure where completely the evidences can be found.

Mohite, M. P et al[2]In the current years the number of cyber crimes is increasing. Forensic investigator requirements to deal with these crimes so they essential particular powerful tools to handle the condition. There are numerous desktop based tools are accessible there is essential develop the forensic tools for cloud as investigator can access the tool somewhere and can store data on the cloud. The simple study of the prerequisite for emerging the computer forensic tool in a cloud computing setting have been mentioned in this paper.

Khan, S et al [3] in this research work investigates the numerous important forensic challenges of MCC which has to address in instruction to classify intruders. Furthermost of these contests are due to virtualization and the dispersed features of MCC. Digital investigators are delimited to finite limits in MCC in the study process. Though, a legally standardized rule requirements to be developed to resolve problems faced by digital investigators in the MCC paradigm. Thus, a normal body has to be recognised to monitor activities done the implementation of policies &implementation of events providing to the domains.

Eleyan, A et al[4] The virtual nature of cloud computing is pushing digital forensics into a novel horizon. Numerous tests are existing in the cloud with jurisdictional and nominal issues. proposes forensic procedure that contains of four phases: Identification, Collection and acquisition, Examination and analysis and consequence dissemination. This paper presents abstract model of forensic procedure as a service (FPaaS) expending cloud-based BPEL. Additional works are essential to grow every service in the forensic procedure and implement FPaaS.

Alex, M. E et al[5]The investigators depend on Cloud Service Provider (CSP) for the data collection. In SaaS and PaaS only high level of logging information can be retrieved by the investigator. In PaaS customers can build their own request so that they possess convinced additional information than SaaS for forensic investigation. High constraint is providing for SaaS customers. IaaS have additional control than the additional two models. In IaaS customer has contact up to the operating system level.

Bachane, I., et al [6] in this paper, we deliberate the readiness for the digital forensic study in a cloud environment, and the challenges faced. Lastly present a novel method for storing and expending evidences in the cloud. propose to implement this method and test particular use cases to make sure its feasibility.

## 3. Proposed Methodology

Nowadays, the web is the major means used by cyber-criminals to carry out attacks alongside People and group. Due to the continually increasing number of Internet users and, as effect, users, these attacks might influence from an enormous goal surface. Characteristic attacks commit during the phishing, online fraud, scamming and so on. In particular, the last years have seen the growing of a threat called data sending or receiving. A data sending or getting attack can be recapitulate as follows:A victim visits a network. The network enclose malicious code intended at exploit vulnerabilities of the customer. If the develop succeed, a malicious binary (characteristically a bot) is downloaded and executed on to the victim's machine. At this point, the attacker increase occupied control of the victim's machine.

In the preceding few years, drive-by data sending or getting attacks have grown into difficult, readily extensible contexts that fit in numerous activities at the similar time and are enormously configurable. In challenging, they effect web technologies in organise the victim's machine and to form, at runtime, the suitable response to be sent to the client. Provide a deep understanding into this problematic, and recommends narrative resolutions for the investigation of existing web-based attacks.

The action have to close to the vendor concerned in data management, done legal and security necessities, based on the information or data that is being stored or transacted. The endeavor has to take each step to protect the effects and furthermore secure its information. There are legal department that get concerned in this process in portion the effort to secure its information. The legal necessities are complete a part of the produce contact with by the enterprise. The commerce in selected event has to variety sure that the vendor is gathering up with the necessities. Created on the location constriction the research was separated into two phases. In the major phase a prototype called trust monitoring system was organised on the provider server. In the aquantity of freeware cloud tools were analysed for suggestion using conservative forensic apparatus at the client side. At the provider side, as a insurance previously cure, a forensic server which acts like a trust monitoring system was deploy.

The scheme logs and audits cloud action infrequently to provide resolution to the non-existent data in the cloud. The forensic server delivers indication of observation to vendor or court judges when a crime is devoted in the cloud.

To overcome the below enumerated issues in web data analysis and pattern detection essential to strategy a novel data model by which the problem is content. To assess the huge scale data a search algorithm is appropriate. Consequently, computation neural network is used for frequent pattern analysis. Though, to handle this huge quantity of log genetic algorithm is comparatively slow process. On the additional hand the accessible data contains the quantity of unique web pages and their access patterns thus, essential to enhance the algorithm by pre-processing of the data. Consequently, MCNN is useful to keep in track the selection procedure. That algorithm supports to discovery the duplicate data patterns after the accessible set of data. For analysing the nearest data patterns completed quantity of session algorithm uses the Euclidian distance and the comparable data is removed from the data set. This procedure reduces the quantity of data for evaluation.

Input :Numerous device raw data(Usage data)
For ($dataset_1$, $dataset_2$,$dataset_3$…data $set_n$)
Step 1. Compute time essential for data transfer one note to another note.
Step2. Recurrent till all data inputs are deliberates

Step3. Assess obtain able abilities in contradiction of resources
Step4. Return value
Step5.Sharingextra resource for existing case
Step6. ifessential
Distribution additions resources
Step7.end if
Step8.wait of subsequent case

Our proposed method combines genetic algorithm and computation neural network to improve the classification accuracy of attack detection. We used computation neural network exploration as a goodness quantity to prune redundant and inappropriate packet, and to rank the packet which contribute additional towards classification. Least ranked packet are removed, and classification algorithm is constructed based on assessed data. This classifier is trained to categorise data set as attacker. Our proposed algorithm contains of two Phase.

First phase: Main part deals with assess attributes expending computation neural network search
Second Phase: two deals with building classifier and quantity accuracy of the classifier

**Proposed Algorithm**
Step 1) load the data set
Step 2) be suitable genetic search on the data set
Step 3) classified the attributes are ranked based on their value
Step 4) excellent the divider of higher ranked data set
Step 5) Apply computation neural network on the subset of attribute that maximizes Classification accuracy
Step 6) calculate precision of the classifier, which actions the capability of the

Classifier to suitably classify unidentified sample.
Step 1 to 4 comes below part 1 which deals with qualities and their position. Step 5 is use to concept the classifier and step 6 proceedings the accuracy of the classifier. Correctness of the classifier is compute as Accuracy = no. Of model appropriately classified in test data

Total no. of illustration in the test data
Specified the significance of the topic, increasing concentration is emerging between forensic practitioners to cloud computing implications to digital forensics. Within few years, the demand for processing digital tasks "as-a-service" will possibly increase amongst practitioners and investigators who will knowledge this novel technique of performing forensic investigations.

## 4. Conclusion

Security exemplify up as a most significant concern in cloud computing. In detail, frequent threats might concern the service or the resolution amongst users and provider. Regardless of the develop of traditional security defense method, cybercrimes on cloud computing infrastructures strength forever happen. To recognise forensics method to assist discovers cybercrime when they do happen. raise such as how to accumulate data, where and how to store metadata for each transaction, how to assess log files, how to categorise attacks on cloud infrastructure. In this research to evaluate the problem of forensics in cloud computing and devise effective explanation to permit for proficient investigation of cybercrimes in cloud compute environment. To overcome these limitations, developed version of computation neural network is proposed in this research. Our proposed method advance classification performance computation neural network is collective with CNN.

## References

[1] Hraiz, S. (2017). Challenges of digital forensic investigation in cloud computing. 2017 8th International Conference on Information Technology (ICIT). doi:10.1109/icitech.2017.8080060.
[2] Mohite, M. P., &Ardhapurkar, S. B. (2015). Overcast: Developing Digital Forensic tool in cloud computing environment. 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). doi:10.1109/iciiecs.2015.7193220.
[3] Khan, S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A. W. A., &Bagiwa, M. A. (2014). Forensic challenges in mobile cloud computing. 2014 International Conference on Computer, Communications, and Control Technology (I4CT). doi:10.1109/i4ct.2014.6914202.
[4] Eleyan, A., &Eleyan, D. (2015). Forensic Process as a Service (FPaaS) for Cloud Computing. 2015 European Intelligence and Security Informatics Conference. doi:10.1109/eisic.2015.14
[5] Alex, M. E., & Kishore, R. (2016). Forensic model for cloud computing: An overview. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). doi:10.1109/wispnet.2016.7566345.
[6] Bachane, I., Adsi, Y. I. K., &Adsi, H. C. (2016). Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. 2016 Third International Conference on Systems of Collaboration (SysCo). doi:10.1109/sysco.2016.7831327.
[7] Ahmad, S., Saad, N. L., Zulkifli, Z., &Nasaruddin, S. H. (2015). Proposed network forensic framework for analyzing IaaS cloud computing environment. 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC). doi:10.1109/ismsc.2015.7594043.
[8] Morioka, E., &Sharbaf, M. S. (2016). Digital forensics research on cloud computing: An investigation of cloud forensics solutions. 2016 IEEE Symposium on Technologies for Homeland Security (HST). doi:10.1109/ths.2016.7568909.
[9] Mthunzi, S. N., Benkhelifa, E., Jararweh, Y., & Al-Ayyoub, M. (2017). Cloudlet solution for digital forensic investigation of multiple cases of multiple devices. 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). doi:10.1109/fmec.2017.7946437.
[10] C.-T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card," IET Inf. Secur., vol. 7, no. 1, pp. 3–10, 2013.
[11] M. B. W. Kobus, P. Rietveld, and J. N. Van Ommeren, "Ownership versus on-campus use of mobile IT devices

by university students," Comput. Educ., vol. 68, pp. 29–41, 2013.
[12] J. James and P. Gladyshev, "Challenges with Automation in Digital Forensic Investigations," arXivPrepr. arXiv1303.4498, 2013.