# DAS: A Novel Approach to Gather Evidence from Cloud

**Gauri Bahirat[1], Kajal Shinde[2], Shital Dudhane[3], Prof. Roma Kudale[4]**

*[1,2,3] Department of Computer Engineering, STES Smt. Kashibai Navale College of Engineering, Vadgaon bk, Pune-41*
*[4] Asst Prof. Department of Computer Engineering, STES Smt. Kashibai Navale College of Engineering, Vadgaon bk, Pune-41*

---

**Abstract—** *Digital forensics have plenty of applications. Digital evidence in the field of forensic investigation has become very important. There are many issues in dealing with network evidence. As network is volatile in nature it becomes difficult to gather network evidence. Sometimes, such information may change with the time, may be located on server which needs authority to get access or far away from the crime scene. In this paper, A novel methodology is presented to collect network evidence. Precisely, the online services like web pages, chats, photos or videos would be source for collecting information. This method is suitable for both experts and non-experts as it takes user through whole process of obtaining evidences. During this process, the information received from remote source is automatically gathered. This information consists of network packets and any information generated by user. A trusted-third party, works as a digital notary to verify both, obtained evidence and the acquisition process.*

**Keywords: Digital Forensics, Network Forensics, Live Network Evidence(LNE), Big Data Forensics, Digital Investigations.**

## 1. INTRODUCTION

Digital forensic has become very important now-a-days, but there are several issues while dealing with network evidence As network is volatile in nature it becomes difficult to gather network evidence. Proposed system should be able to collect information regarding requested topic from data stored on cloud. This information is acquired using three operation modes namely, LNE-Proxy, LNE-Agent, Savvy users. These three OMs ensures verified data is collected. After collection of this data evidence packing process is carried out in order to preserve the integrity of data. Packing process consist of encryption and providing digital signature to gathered evidences. The system can be used for collection of evidences of a kind who's integrity cannot be questioned.

## II. LITERATURE REVIEW

**Cloud incident handling and forensic-by-design: cloud storage as a case study :**

In this paper an integrated cloud incident handling is done with the Information security incident handling strategies or models are important to ensure the security of organizations, particularly in cloud and big data environments. However, existing strategies or models may not adequate as cloud data are generally virtualised, geographically distributed and ephemeral, presenting both technical and jurisdictional chal-lenges. They present an integrated cloud incident handling and forensic-by-design model. But limitations of this system is deploying the proposed mode in a real world setting,with the aims of validating and refining the model.

**Cloud Infrastructure Resource Allocation for Big Data Applications :**

In this paper they Increasing popular big data applications bring about invaluable information, but along with challenges to industrial community and academic things only. Cloud computing with unlimited resources seems to be the way out. However, if we do not arrange fine allocation for cloud infrastructure resources then this panacea cannot play its role. In this paper, they present a multi-objective optimization algorithm to trade off the performance, availability, and cost of Big Data application running on Cloud. After analyzing and modeling the interlaced relations among these objectives, they design and implement there approach on experimental environmentbut the limitations of this system are, First one is to add more constraints, including the security and data processing preference. The second one is to test our approach on advanced networking environments, such as Software-Defined Networking (SDN).

**Cloud Storage Forensic: hubiC as a Case-Study :**

In this project by using cloud services, users can access files anywhere with an internet connection. This paper presents investigation of hubiC as one of popular cloud platforms running on Microsoft Windows 8.1. Remaining artfacts per-taining different usage of hubiC namely upload, download, installation and uninstallation on Microsoft Windows 8.1 are presented. But limitations of this system is Direct future applications of this research could apply similar methodology to the investigation of other cloud platforms, (e.g. ADrive, eCloud, etc) on Windows 8.1. This would increase the scope of the investigation and provide greater insight to an investiga-tor, potentially revealing common flaws across several cloud platforms.

Cloud storage forensics: own Cloud as a case study: Using own Cloud as a case study, we successfully undertook a forensic examination of the client and server components of an own Cloud installation and discussed the relevance of a number of artifacts to a forensic investigation. and the Limitations of this system is, Further work on the potential for network interception as a method of forensic collection should be pursued especially as a method of identification of potential evidence sources.

**Digital droplets: Microsoft SkyDrive forensic data remnants. :**

To find that an examiner can identify SkyDrive account use by undertaking keyword searches, hash comparison, and examine common file locations in Windows 7 systems to locate relevant information. and Limitations of this system is, A future research opportunity would be to undertake the experiments with the Windows 8 operating system to determine if the same data remnants are present. Future research opportunities include conducting research in to the remnants of other cloud storage services such as Google Drive.

The above mention systems have some drawbacks. This paper proposes a new method which overcomes the above stated applications drawbacks.

Evidence acquisition has attained a lot of focus in recent times, few approaches among them as listed below,

There's an approach [1] in which, cloud computing with unlimited resources seems to be the way out. However, this panacea cannot play its role if we do not arrange fine allocation for cloud infrastructure resources. In this paper, they present a multi-objective optimization algorithm to trade off the perfor-mance, availability, and cost of Big Data application running on Cloud. After analysing and modelling the interlaced rela-tions among these objectives, they design and implement their approach on experimental environment but the limitations of this system are, first one is to add more constraints, including the security and data processing preference. The second one is to test our approach on advanced networking environments, such as Software-Defined Networking (SDN).

Another approach cloud incident handling [10] and forensic-by-design: cloud storage as a case study, this paper an inte-grated cloud incident handling is done with the Information security incident handling strategies or models are important to ensure the security of organisations, particularly in cloud and big data environments. However, existing strategies or models may not adequate as cloud data are generally virtualised, geo-graphically distributed and ephemeral, presenting both techni-cal and jurisdictional challenges. They present an integrated cloud incident handling and forensic-by-design model. But limitations of this system are deploying the proposed mode in a real-world setting, with the aims of validating and refining the model.

There is a survey conducted [3] by using cloud services, users can access files anywhere with an internet connection. This paper presents investigation of hubiC as one of popular cloud platforms running on Microsoft Windows 8.1. Remaining artefacts pertaining different usage of hubiC namely upload, download, installation and uninstallation on Microsoft Windows 8.1 are presented. But limitations of this system are Direct future applications of this research could apply similar methodology to the investigation of other cloud platforms, (e.g. ADrive, eCloud, etc) on Windows 8.1. This would increase the scope of the investigation and provide greater insight to an investigator, potentially revealing common flaws across several cloud platforms.

## III. MOTIVATION AND OBJECTIVE

### A. MOTIVATION

The motive of the project is to obtain information from trusted third party which collects information on behalf of investigator by using Live Network Evidence method. The investigator establishes the connection with TTP. This connection is secured to maintain privacy.

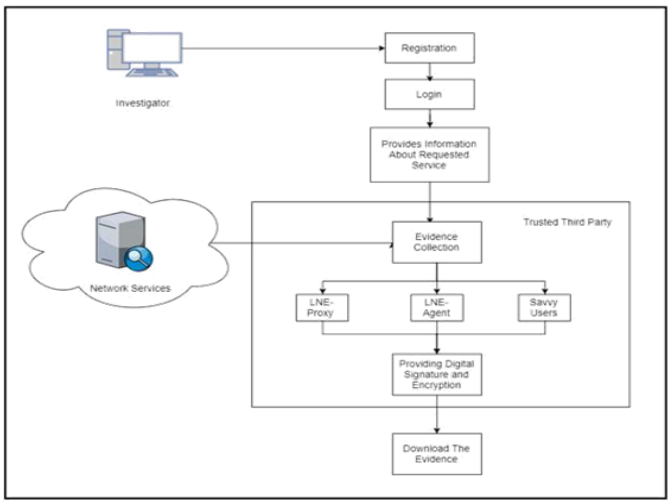
### B. OBJECTIVE

Previous acquisition tools proposed in the last years suffer from various limitations. Firstly, they typically lack of non-repudiation and data-integrity solutions to protect the collected information, which means that the result of the investigation could be interfere by an attacker. Also, we cannot be assured about reliability of source of information. Lastly, this type of acquisition processes was vulnerable to 'man-in-the-middle' attack. So, we proposed a method through which we can get the reliable and valid data.

## IV. PROPOSED SYSTEM

We present a LNE method to obtain information from network in such a way that the integrity, authenticity and origin of the data can be guaranteed. TTP uses network services which are used for collecting information from online service on behalf of investigator. The investigator starts this acquisition process by establishing connection with TTP. This connection is secured to maintain confidentiality and integrity of data being transferred and also to maintain privacy of involved parties. TTP provides communication medium through which investigator carry out the acquisition process. The LNE method works in three operating modes(OM) i.e. LNE-Proxy, LNE-Agent, savvy users.

## V. SYSTEM ARCHITECTURE




We present a method to obtain information from network in such a way that the integrity, authenticity and origin of the

data can be guaranteed. TTP uses network services which are used for collecting information from online service on behalf of investigator. The investigator starts this acquisition process by establishing connection with TTP. This connection is secured to maintain confidentiality and integrity of data being transferred and also to maintain privacy of involved parties. TTP provides communication medium through which investigator carry out the acquisition process. The LNE method works in three operating modes(OM) i.e. LNE-Proxy, LNE-Agent, savvy users. A trusted third-party data acquisition system is proposed. This system will collect the evidences and provide digital signature, Encryption to preserve integrity of data. Thus, once the data is acquired by system, it can be considered that the collected data is not only authenticated but also the digital signature ensures that it is robust against attacks like spoofing or man-in-the-middle attack. The system will work in three operating modes:

### A. LNE-Proxy

In this mode of operation, information related networks, servers, etc. is collected. This information can be used in order to identify attacks like man-in-the-middle and spoofing etc.

### B. LNE-Agent

Number of different sources collect information regarding requested topic/incident. This information then put under process of finding co-relations to extract relevant content. This operation mode thus, verifies source of information.

### C. Savvy Users

In above two modes of operation, investigator does not par-ticipate in investigation process unlike third operation mode.

## VI. CONCLUSION

The idea of acquisition of Live Network Evidence (LNE) from online services is based on Trusted-Third-Party (TTP). TTP collects the information on behalf of investigator. Data will be obtained by using three different modes. The evidence collected by TTP are strong and its validity can be checked at any time after acquisition process. This data is more accurate and its integrity and authenticity can be guaranteed.

## VII. ACKNOWLEDGEMENT

With due respect and gratitude, We take the opportunity to thank those who have helped us directly and indirectly. We convey our sincere thanks to Dr. P. N. Mahalle, Head Department of Computer Engineering and Prof. Roma Kudale for their help in selecting the project topic and support. We thank to our project guide Prof. Roma Kudale for her guidance, timely help and valuable suggestions without which this project would not have been possible. Her direction has always been encouraging as well as inspiring for us. Attempts have been made to minimize the errors in the report. We would also like to express our appreciation and thanks to all our friends who knowingly or unknowingly have assisted and encourage us throughout our hard work. Finally how can We forget the almighty the supreme power the GOD and our loving parents without which this work task was a distant dream.

## REFERENCES

1. W. Dai, L. Qiu, A. Wu, and M. Qiu, Cloud Infrastructure Resource Allocation for Big Data Applications, IEEE Transactions on Big Data, vol. PP, no. 99, pp. 11, 2016.

2. NIST, Disk imaging tool specification, Computer Forensics Tool Testing (CFTT) Project, Tech. Rep., 2001.

3. B. Blakeley, C. Cooney, A. Dehghantanha, and R. Aspin, Cloud Storage Forensic: hubiC as a Case-Study, in 7th IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2015, Vancouver, BC, Canada, November 30 - Dec. 3, 2015. IEEE Computer Society, 2015, pp. 536541. [Online]. Available: http://dx.doi.org/10.1109/CloudCom.2015.24

4. National Institute of Justice (USA), Digital Forensics Standards and Capacity Building, (Available from: http://nij.gov/topics/forensics/evidence/digital/standards/welcome.htm), [Accessed on 17 October 2012].

5. W. Kruse and J. Heiser, Computer Forensics: Incident Response Essentials. Pearson Education, 2001. [Online]. Available: http: //books.google.it/books?id=-qWa5Svv7BIC

6. Sheetz, Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers. Wiley, 2007

7. D. Quick and K.-K. R. Choo, Digital droplets: Microsoft Sky Drive forensic data remnants, Future Generation Computer Systems, vol.29, no. 6,pp.13781394, 2013.[Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X13000265

8. Google Drive: Forensic analysis of data remnants, Journal of Network and Computer Applications, vol. 40, pp. 179 193, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804513002051

9. L.Wang, S. Tasoulis, T. Roos, and J. Kangasharju, Kvasir: Scalable Provision Of Semantically Relevant Web Content on Big Data Framework, IEEE Transactions on Big Data, vol. PP, no. 99, pp. 11, 2016.

10. N. H. Ab Rahman, N. D. W. Cahyani, and K.-K. R. Choo, Cloud incident handling and forensic-by-design: cloud storage as a case study, Concurrency and Computation: Practice and Experience, pp. n/an/a, 2016. [Online]. Available: http://dx.doi.org/10.1002/cpe.3868