Design And Development Of Multi-Stream Cloud Forensic Technique

Mr.Kalyan Devappa Bamane , Dr Dinesha H.A
,

Abstract: A proposed multi-stream forensic technique for performing forensic investigations in an electronic system includes capturing and associating multiple streams of information. The multi-streams refer network stream, storage stream, and virtual stream. The network stream contains a record of network activities such as traffic data, server logs, host activities details, and firewall data so on. A storage stream refers to data of storage media such as hard disk, memory, flash drive, and network area storages which record both read and write activities. A virtual stream refers to data of virtual machines, virtual servers, virtual memory, virtual drives and related sources. A comprehensive summary logs can be obtained with each network, storage, and virtual activities coordinated during particular time. To enable investigation for finding the suspicious events across network, storage, and virtual domains multi-stream forensic technique has been proposed. It achieves cloud security breach investigation and recovery. Proposed framework refers multiple stream sources and logs for investigation through identifying the footprint and recovering the data.

Index Terms: Cloud security, Cloud Forensic, Investigation, Multi-Stream, Technique, Cyber, Virtual domain

1. INTRODUCTION

Cloud forensics technology is a combined platform of cloud computing technology and digital forensics techniques [1]. Cloud computing can be defined as a shared collection of configurable network components and resources such as networks, servers, storage, applications and services that can be reconfigured and built up dynamically with minimal effort [2]. Digital forensics is the technique of computer science principles to investigate and recover digital proof for the diagnosis and prosecution [3][4]. Cloud forensics is a part of internet and network forensics. It deals with forensic investigations of internet and networks. Cloud computing is works on wide network and resource access. Consequently, cloud forensics tracks the main stages of network forensics with techniques personalized to cloud computing environments. Multi-jurisdictions and multi-tenancy are the default settings of cloud forensics, that make additional legal challenges [5][6]. Sophisticated interactions between CSPs and customers, resources sharing by more than one tenants and collaboration between worldwide law enforcement organizations are required in most cloud forensic investigations. The technical size encompasses the approaches and tools which might be needed to carry out the forensic method in a cloud computing surroundings [7]-[10]. These encompass information series, live forensics, proof segregation, virtualized environments and proactive measures. Statistics collection is the procedure of figuring out, labelling, recording and obtaining forensic statistics. The forensic facts consist of customer-side artefacts that are living on customer premises and cloud service provider-facet artefacts which are placed inside the company infrastructure. The tactics and equipment used to acquire forensic records vary primarily based on the particular model of facts responsibility this is in vicinity.

- *Kalyan Devappa Bamane, Department of Computer Science and Engg. VTU Belgavi India . Email:kalyandbamane@gmail.com*
- *Dr.Dinesha H.A, Department of Computer Science and Engg. VTU Belgavi India . Email:sridini@gmail.com*

The collection method must hold the integrity of statistics with sincerely described segregation of responsibilities among the purchaser and provider. It should not breach laws or rules in the jurisdictions where information is accumulated, or compromise the confidentiality of other tenants that proportion the resources. Speedy elasticity is one of the important characteristics of cloud computing. Cloud sources may be provisioned and de-provisioned on call for [11]. As an end result, cloud forensic tools also need to be elastic. In most cases, those consist of huge-scale static and live forensic equipment for records acquisition (such as unstable information collection), facts recovery, evidence examination and evidence analysis. Another critical characteristic of cloud computing are resources pooling [12]. Multi-tenant environments lessen IT expenses thru resources sharing. However, the method of segregating proof in the cloud requires compartmentalization [4]. For this reason, strategies and tools ought to be advanced to segregate forensic statistics among multiple tenants in numerous cloud deployment models and service fashions. Virtualization is a key technology that is used to implement cloud services. However, hypervisor research techniques are almost non-existent. Every other task is posed by means of the lack of facts control [4]. Techniques, algorithms and tools ought to be developed to physically discover forensic records with precise timestamps while considering the jurisdictional troubles [13]. Hence, the effort towards investigating the cloud forensic techniques has made and proposed the multi-stream cloud forensic techniques. It collects process, analyse and recover through multiple streams and logs. This paper has been organised in the following manner. Section 2 describes system design; section 3 describes development of proposed system. Section 4, presents the conclusion with future enhancements.

1. System Design

This section describes the design details of proposed the multi-stream forensic technique. As presented in figure 1, multi-stream technique connects with multiple streams such as network stream, storage stream and virtual stream to gather the logs data. Further, these data will be processed and kept in database for ready analysis against the attacks.

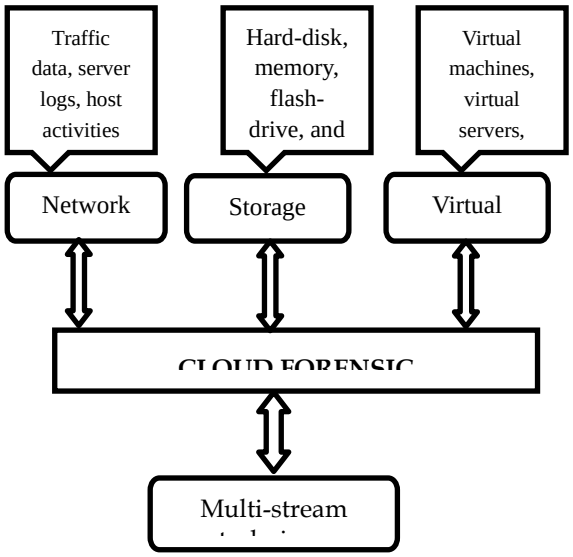

***Figure 1**: Multi-stream cloud forensic technique*

On suspecting attacks, this technique gets active automatically for analysing, reporting and recovering the data. Figure 2, represents the proposed different process of proposed technique. It performs the data log collections, hasing, analysis, reporting, and recovering the process.

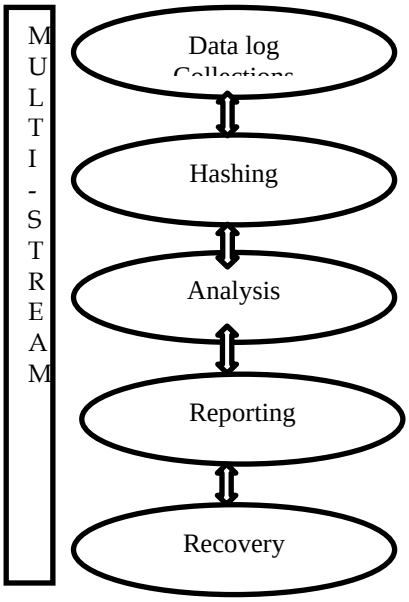

***Figure 2:** Multi-stream technique process*

2. SYSTEM DEVELOPMENT

This section describes the development details of proposed multi-stream technique. The proposed algorithm1 describes the steps of multi-stream techniques, where in which the identifying, connecting, and calculation of multiple streams can be performed to keep the backup evidence information against attacks. Hashing will be performed on step 3 to keep hashing value at data base. In step 4, analysis for attack and continuous monitoring will be done. Step 5, reports against the suspicious activities through predefined technique. Step 6, submit the evidence and recover the data attacks.

Algorithm 1: Multi-stream technique
Step1: Start the technique by identifying the multiple streams of cloud enabled system
MST->ms_1, ms_2, ms_3….. ms_n

Step 2: Connecting to all identified streams and determines its sources for collecting logs
ms1 (l_1, l_2, .. ln) , ms2 (l_1,l_2,.. l_n) and m3 (l_1,l_2,…l_n)

Step3: Calculation of Hash values and stores the same at backend database
H_1<- hf(ms1(l_1,l_2,…l_n) , ms2 (l_1,l_2,..l_n) and m3 (l_1,l_2,…l_n))
H_2<- hf(ms1(l_1,l_2,…l_n) , ms2 (l_1,l_2,..l_n) and m3 (l_1,l_2,…l_n))
H_n<- hf(ms1(l_1,l_2,…l_n) , ms2 (l_1,l_2,..l_n) and m3 (l_1,l_2,…l_n))
Dbase <- H_1, H_2,… H_n

Step 4: Analysis of cloud sources for attack footprint
Analysis (Dbase) with Calculated Hash (Cloud data)
Set malicious flag mf=1 on mismatch
Else
Set malicious flag mf=0

Step 5: Report against suspicious activities
If mf=1 then
Report to automated system, prepare evidence and invoke recovery system
Invoke (Report & Recovery)
Else
False positive counter increment
End if
Report ()
Set Communication <- Email/SMS/alert signal to Concerned
Recovery ()
Connect to Dbase <- H1, H2, .. Hn
Determine the logs l1,l2…ln
Reproduce the data using digital forensic methods against ms1 (l_1, l_2,…l_n) , ms2 (l_1,l_2,..l_n) and m3 (l_1,l_2,…l_n))

Step 6: Submit evidence and recover the data for reliability
Proposed framework refers multiple stream sources and logs for investigation. It has various processes such as collection, hashing, analysis; reporting and recovery which can be executed against identified multiple streams of the system. Major streams are network, storage and virtual systems. These systems individual components can be connected analysed and recovered against attacks. Design of multi-stream technique has been presented and discussed. Development algorithm for attaining the investigation, reporting and recovery has been described. This technique helps the cloud service provider and customer on active and passive attacks. If any cloud data deleted, modified and changed, it identifies and reproduce the original content at high probability. Evaluation of proposed technique with respect to probability of reporting attacks and probability of recovering the data will be the future focus of our research.

.

Acknowledgment

REFERENCES

[1] N. Beebe, V, G. Peterson and S. Shenoi (Eds.)," Digital forensic research: The good, the bad and the unaddressed, in Advances
[2] in Digital Forensics ", Springer, Heidelberg, Germany, pp. 17–36, 2009
[3] R. Broadhurst," Developments in the global law enforcement of cybercrime, Policing", IJPSM-International Journal of Police
[4] Strategies and Management, vol. 29(2), pp. 408–433, 2006
[5] Cloud Security Alliance: www .cloudsecurityalliance.org/csaguide.pdf,
[6] "Security Guidance for Critical Areas of Focus in Cloud Computing
[7] V2.1", San Francisco, California, 2009.
[8] EurActiv, "Cloud computing: A legal maze for Europe, Brussels, Belgium ", 2011
[9] Heraklion, Crete, Greece (), www.enisa.europa.eu/act/rm/files
[10] /deliverables/cloud-computing-risk-assessment, Cloud Computing:
[11] Benefits, Risks and Recommendations for Information Security,
[12] "ENISA - European Network and Information Security Agency" 2009
[13] www .rcfl.gov/downloads/documents/RCFL Nat Annual07.pdf , "
[14] Federal Bureau of Investigation, Regional Computer Forensics
[15] Laboratory, Annual Report for Fiscal Year ", Washington, 2007
[16] www.gartner.com/it /page.jsp?id=920712, Gartner, Gartner says
[17] worldwide cloud services revenue will grow 21.3 percent in
[18] 2009, Stamford, Connecticut, March 26, 2009
[19] F. Gens, IT cloud services forecast – 2008 to 2012: A key driver of new
[20] growth, October 8, 2008
[21] K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating
[22] Forensic Techniques into Incident Response, Special Publication 800-
[23] 86, NIST, Gaithersburg, Maryland, 2006
[24] S. Liles, M. Rogers and M. Hoebich, V, G. Peterson and S. Shenoi (Eds.) , "A survey of the legal issues facing digital
[25] forensic experts, in Advances in Digital Forensics", Springer, Heidelberg, Germany, pp. 267–276, 2009.
[26] P. Mell and T. Grance, "The NIST Definition of Cloud Computing
[27] (Draft), Special Publication 800-145 (Draft), NIST, Gaithersburg,
[28] Maryland, 2011
[29] Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, Chapter 2, CLOUD FORENSICS, 16-26.