ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Cloud Forensics: Need for an Enhancement in Intrusion Detection System

Jyoti Chaudhary[1]
Dept. of Computer Science
DIT University
Dehradun, India.

Dr. Rama Sushil[2]
Dept. of Computer Science
DIT University
Dehradun, India.

Abstract: ***Digital forensics in cloud computing and storage is consistently gaining its importance as one of the most important challenge due to cyber and computer assisted crime. Whilst the existence of many tools and research, the future of forensic investigation is yet to be established. This paper examines, the cloud forensic tools, challenges posed by forensic investigators, Intrusion Detection System and presents a systematic approach to support the investigation while enhancing the Intrusion Detection System.***

Key Words: alert correlation; cloud computing; cybercrime; computer forensics; cloud web services; intrusion detection system.

I. INTRODUCTION

With the time, cloud computing has emerged as the most vital and fast-growing model in the IT industry facilitating the group collaboration and computing as a service rather than a product. In recent years, an explosion has been seen in the number of cloud computing applications. Small and medium scale industries find cloud immensely cost effective as it offers the scalable pay-as-you-go service. Khajeh-Hosseini et al. [1] analyzed that 37% of cost could be saved if organization migrated its outsourced datacenter to Amazon's Cloud. Clouds use virtualization model to ensure better resource utilization. Cisco GCI [2] forecasts that global data center traffic will be 7.7 zettabytes annually in 2017 representing a 25% CAGR with Asia Pacific as the highest traffic growth region representing a 43% CAGR. More than half of survey respondents say their organization currently transfers sensitive or confidential data to the cloud [3]. With big data storage and more enterprise migration to cloud, comes cloud forensic challenge.

In a survey by IDC IT Cloud Services, 74% of IT executives and CIOs cited security as the main reason preventing their migration to cloud services model [4]. Rapid increase in the number of attacks on cloud services like Dropbox, Basecamp, iCloud, Feedly, Evernote, Tumblr, IFTTT, Google Drive, Microsoft's Lync, Microsoft's Exchange, AWS, Samsung's Smart TV has driven the concern of forensic experts to focus on new tools and techniques for digital forensics [5]. 36% annual rate increase in cloud market analyzed, PR news. Analysts expected AWS revenues to hit $6 billion - $10 billion in 2014. Microsoft Azure was predicted to reach $1 billion in the annual sales in 2014. Oracle Cloud bookings increase by 35% in the 3rd quarter in 2014. Gartner predicts 60% of banking institutions to migrate to the cloud. By 2018, global market for cloud equipment will reach $79.1 billion as per predicted reports. More than $180 billion is expected to be spent by the end-user in 2015 [6].

II. BACKGROUND

A. Cloud computing

The Open Cloud Manifesto Consortium defines cloud as "the ability to control the computing power dynamically in a cost efficient *way and the ability of end-user, organization, and It staff to utilize the most of that power without having to manage*

the underlying complexity of the technology" [7]. Cloud computing essential characteristics are on-demand self service, resource pooling, broad network access, rapid elasticity, measured service, multitenancy, productivity, performance.

B. Cloud deployment models

Cloud has following four models:

- Private Cloud: Designed only for a particular enterprise. It can be hosted internally or externally, managed by third-party or internally. It offers greater control and focuses more on data security. There are two variations for private cloud [8]:
  - On-premise Private Cloud: Also referred as internal clouds, are hosted within enterprise's own data center, and is limited in terms of scalability and size.
  - Externally hosted Private Cloud: Hosted externally with a cloud provider which guarantee privacy.
- Public Cloud: Serves multiple tenants and provides pay-per-usage model. It offers services open for public use, but operated and owned by third party. Examples of such providers are Amazon AWS, Microsoft and Google.
- Hybrid Cloud: Composition of two or more than two clouds from different service providers.

C. Cloud service models

It has three service models, i.e., Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS).

- SaaS: Highest level service provides the access to application software often referred to as on-demand software. Examples: Google Apps, Microsoft Office 365, Hotmail, Gmail.
- PaaS: Provides the computing platform, typically including operating system, programming language execution environment, database, web server. Developers after developing their software solutions, run it on cloud platform. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.
- IaaS: Provides the computing infrastructure and platform (virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks) to allow cloud user to run applications on their own computers, physical or virtual machines and other resources like Examples: Amazon EC2, Windows Azure, Rackspace, Google Compute Engine.

Many other delivery models have been proposed like Taas, The table 1 given below shows some top cloud services according to the Skyhigh cloud adoption risk report q2 2014. Table 2 shows some top file sharing, collaboration, and social media cloud services [9].Various other delivery models have been suggested by other researchers like desktop as a service (DaaS), IT as a service (ITaaS) [10], Confidentiality as a service (CaaS) [11] and many more.

File Sharing	Collaboration	Social media
Dropbox	Office 365	Facebook
Google Drive	Gmail	Twitter
Box	Cisco Webex	LinkedIn
OneDrive	GoogleDocs	Seina Weibo
eFolder	Prezi	Tumblr

Table 2: Some top services by category

Top 10 enterprise cloud services	Top 10 consumer cloud services
Amazon Web Services	Facebook
Office 365	Twitter
Salesforce	Apple iCloud
Cisco Webex	Youtube
Box	Linkedln
Yammer	Dropbox
ServiceNow	Gmail
SuccessFactors	Google Docs
Adobe Echosign	Pinterest
Liveperson	Instagram

Table 1: Top 10 consumers and enterprise cloud services

III. CLOUD FORENSIC

A. *Challenges*

Cloud forensic is cross-disciplinary between digital forensics and cloud computing [12]. To investigate the crimes in the cloud environment, forensic experts have to carry out a digital forensic investigation. Digital forensics definition acc. to NIST: "*Digital forensics is the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data"* [13]. Cloud forensics has been divided into three dimensional [14] challenges:

- Technical dimension – involves media collection, data examination, information analysis, evidence reporting. It has few main areas to focus such as forensic data collection, evidence segregation, investigations in virtualized environment, proactive preparations, elastic, static and live forensics.
- Organizational dimension – involves CSP, and the cloud customer. It has three main areas to focus such as segregation of duties, collaboration, policy.
- Legal dimension – involves jurisdictional issues and multitenancy, service level agreement, multi-ownership.

The data shown in figure 1 and figure 2 on next page, gives statistical analysis of main challenges and main opportunities that exist in cloud forensics. According to a survey conducted by cloud future 2011, Microsoft Research Redmond [15] , Jurisdiction is the topmost challenge in cloud forensics with 90.14% . Most valuable research direction is 88.57% in Designing forensic architecture for the cloud.

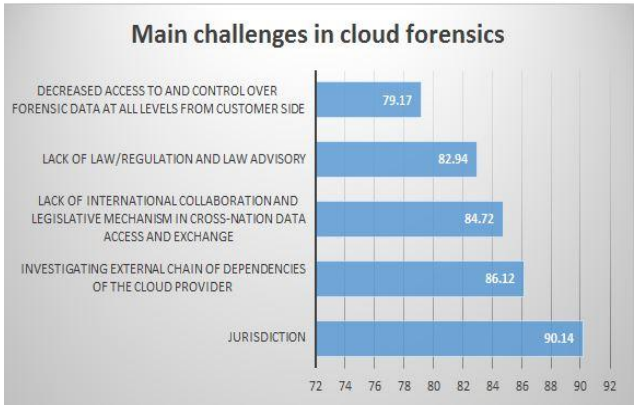

Figure 1: Main challenges

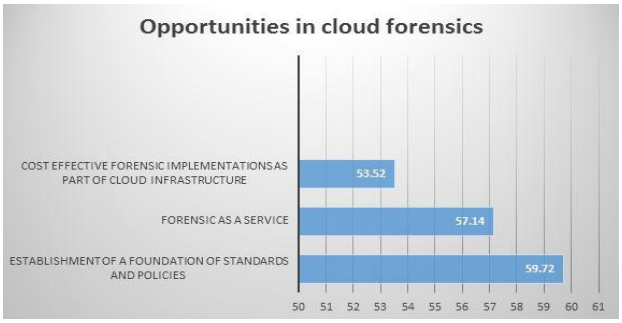

Figure 2: Opportunities in cloud forensics

B. Forensic tools

At present there are over 130 free forensic tools [16] available which include file and data analysis, email analysis, data capture, Mac OS, file viewers, Mobile devices, internet analysis, registry analysis, Application analysis, abandonware, disk tools and many more but still digital forensics is one of the biggest challenge for forensic experts. Some common forensic tools are: EnCase, FTK, Wireshark for cross platform, DECAF, Cofee, X-ways. Cofee is developed by Microsoft. New techniques to prevent cloud crime are yet to be devised and hence poses a great challenge to the emerging paradigm of cloud technology

C. Attacks known on cloud

Type of attacks on cloud	**Attack possible on**
DOS	Network and cloud infrastructure
Theft of service	Cloud infrastructure
Cloud malware injection	Cloud infrastructure
Cross VM side channels	Cloud infrastructure
Targeted shared memory	Cloud infrastructure
Phishing	Cloud infrastructure, network, access
Botnets	Cloud infrastructure, access and network
Audio stegnography	Cloud infrastructure and access
VM rollback attack	Cloud infrastructure and access

Table 3: Possible attacks on cloud

D. IDS Issues

IDS monitor network or system activities for policy violations or malicious activities. IDS are divided into two main categories network based (NIDS) and host based (HIDS) intrusion detection systems. To protect data against network attacks mixed with and generate alerts when malicious or suspicious events are detected. Amongst alerts generated by IDS there are alerts that are false which get mixed with the true ones and thereby making it difficult for users to differentiate between them. There are alerts which IDS may miss; hence there is a need for alert correlation [18]. Gul et al highlights that encrypted data traffic cannot be detected by traditional IDS and Network IDS [19].

Before introducing IDS to an organization, there are several issues to be considered. The entire process is not automated as thought. Werlinger et al [20] call for human interference. Initial installation is complex, needs detailed configuration specific to the organizations network requirements and characteristics [21]. All of this result in an increment in the overall cost [22].

When the IDS is functional, more issues originate. Typical IDS generate log files for later analysis. This again calls for human interference [20]. The issue of storage of very large log files arises. System generated alerts require analysis, which can be performed manually or with the usage of GUI tools [23]. Logs inspection is easier with visual tools, however finer details can be missed that manual inspection is less likely to do. Hours of manual examination may fail sometimes in the inspection of finer details. Indeed a combination of both the methods would appear to be the best possible solution. Log analysis requires

interpretation of key characteristics and determining the earnestness of false positives. As Wagner points out [24] too many false positives detection in the alert log and users may lose overall faith in the IDS.

Configuration of IDS requires technical expertise. IDS is expected to block all potential malicious packets that are detected. Such an action may indeed protect the internal network, but produces possibility of a Denial of Service occurring, whereupon a malicious attacker bombard the network with a large series of malicious packets. Configuring IDS is probable to be on-going throughout the lifetime of the device. IDS rule sets must be modified with change in threats. All this process needs knowledge about organization as well as human interference.

Corona et al highlights Denial of Service and overstimulation and points that attacks coming from outside the network are also possible on IDS [25]. As a result, IDS cannot operate properly and is overwhelmed with false positive and false negative alerts.

E. DHT implementationsin IDS

There are various routing implementations of DHT but famous are Pastry by Microsoft, Chord developed at MIT, Kademlia [26]. Pastry[27], Chord [28] and CAN are second generation Peer-to-Peer applications. Kademlia due to its simplicity has rare chances of improvement due to its parallel routing and better performance. On the other hand Pastry and Chord are more prone to changes due to their complex design, thereby giving chance to researchers to evolve. All these DHT implementations are prone to Sybil attacks [29]. BitTorrent, Napster, Gnutella all these Peer-to-Peer systems use DHTs. Amazon's Dynamo use Chord. Applications like PAST [30] and SCRIBE [31] have been developed on top of Pastry.

IV. Conclusion

This paper presents and evaluates challenges posed by forensic world and opportunities in it. It also presents various DHT routing implementations being used in the Intrusion Detection System. DHT routing implementations like CORD and Pastry have much scope for the improvement in future and work shall be carried out in this field to make the base of IDS strong. Measures must be taken to deal with the arising issues in cloud forensics. The development of new forensic tools must be a good research area for practitioners and researchers to carry out forensics in an efficient way due to breach in confidentiality and data on cloud or a network.

Acknowledgement

I am thankful to my guide Dr. Rama Sushil for her immense support, proper guidance and valuable suggestions throughout this course of my work. I am also thankful to the Head of Computer Science dept., Dr. Garg for giving me the opportunity to learn and my friend anurag for his motivation. I once again extend my sincere thanks to all of them.

References

1. khajeh-Hosseini, D. Greenwoods, and I. Sommerville, "Cloud migration: A case study of migrating an enterprise IT system to IaaS," Proceedings of the 3rd International Conference on Cloud Computing (CLOUD). IEEE, 2010, pp. 450-457.
2. Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2012-2017," Cisco. Retreived from http://www.cisco.com/c/en/us/Solutions/collateral/service-provider/global-cloud-index-gci/cloud-index-gci/Cloud-Index-White-Paper.html. [Accessed 13/10/14].
3. Jack Woods, "20 cloud computing statistics every CIO should know," Silicon Angle. Retreived from http://www.siliconangle.com/blog/2014/01/27/20-cloud-computing-statistics-tc0114/ [Accessed 13/10/14].
4. Clavister, "Security in the cloud,". Retreived from https://www.clavister.com/globalassets/documents/resources/white-papers/clavister-whp-cloud-security-en.pdf Clavister White Paper, [Accessed 13/10/14].
5. Computer World, "The worst cloud outages of 2014," Computer World. Retreived from http://www.computerworlduk.com/slideshow/cloud-computing/3539805/the-worst-cloud-outages-of-2014-so-far/10/ [Accessed 13/10/14].
6. I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, H. Balakrishnan, "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications," in IEEE/ACM, San Diego, California, USA, 20001.
7. Open Cloud Consortium, "Open cloud manifesto," The Open Cloud Manifesto Consortium, 2009.
8. Cattelecom, "Cloud Computing :An Overview,". Retreived from http://south.cattelecom.com/rtso/Technologies/CloudComputing/Cloud-Computing-Overview.pdf.

9. Skyhigh, "Skyhigh Cloud Adoption Risk Report". Retrieved from http://www.Skyhigh.com/Skyhigh-Cloud-Adoption-Risk-Report-Q2-2014a.pdf [Accessed 13/10/14].
10. J. Hine and B. Laliberte, "Enabling IT-as-a-Service," pp. 1–11, 2011.
11. Fahl, Sascha, M. Harbach, T. Muders, and M. Smith. "Confidentiality as a Service--Usable Security for the Cloud," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pp. 153-162. IEEE, 2012.
12. K. Ruan, Prof. J. Carthy, Prof. T. Kechadi, M. crossbie, "Cloud forensics: An Overview", in Centre for Cybercrime Investigation, University College Dublin, IBM Ireland Ltd.
13. K. Kent, S. Chevalier, T. Grance, H. Dhang, "Nist guide to Integrating forensic Techniques into Incident response", NIST, 2006.
14. Cloud Times, "Basics of Cloud Forensics", Cloud Times. Retreived from http://www.cloudtimes.com/The Basics of Cloud Forensics _ CloudTimes.htm [Accessed 13/10/14].
15. K. Ruan, "Cloud Forensics: An Overview,". Retreived from http://research.microsoft.com/en-us/um/redmond/events/cloudfutures2011/slides/friday/security-software_ruan.pdf [Accessed 23/9/14].
16. Forensic Control Ltd, "Forensic Tools", Forensic Control Ltd. Retreived from https://forensiccontrol.com/resources/free-software/ [Accessed 18/2/15]
17. I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey," Computers 3(1), pp. 1- 35, 2014.
18. D. XU, and P. Ning, "Correlation Analysis of Intrusion Alerts," in Springer US, Advances in Information Security Volume 38, pp 65-92, 2008.
19. I. Gul and M. Hussain, "Distributed Cloud Intrusion Detection Model," International Journal of Advanced Science and Technology, vol. 34, pp. 71–82, 2011.
20. R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, and K. Beznosov, "The Challenges of Using an Intrusion Detection System: Is it worth the effort?," in Proc. of the 4th symposium on Usable privacy and security, no. 1, pp 107-118, 2008.
21. "How do I enable two-step verification on my account?" Internet: https://www.dropbox.com/help/363/en, [13/10/14].
22. R. Bhatnagar, A.K. Srivastava, and A. Sharma, "An Implementation Approach for Intrusion Detection System in Wireless sensor Network", International Journal on Computer Science and Engineering (IJCSE), vol. 2, no.7, pp. 2453-2456, 2010
23. C. Pautasso and F. Leymann, "RESTful Web Services vs . ' Big ' Web Services : Making the Right Architectural Decision Categories and Subject Descriptors," pp. 805–814, 2008.
24. D. Wagner, "Intrusion Detection System", Internet: http://www.cs.berkeley.edu/~daw/teaching/cs261-f07/scribenotes/1025-brian.pdf, Oct. 25, 2007 [3/10/2012].
25. I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," Information Sciences, no. March, Mar. 2013.
26. P. Maymounkov, and D. Mazieres, "Kademlia: A Peer-to-peer Information System Based on the XOR Metric," in IPTPS'01: Revised Papers from the First International Workshop on Peer-to-peer Systems. London, UK: Springer-Verlag, 2002, pp. 53-65
27. A. Rowstron, and P. Druschel, "Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems," in Proc. of the 18th IFIP/ACM International conference on Distributed Systems Platforms, Heidelberg, Germany, November 2001.
28. S. Baset, H. Schulzrinne, and E. Shim, "A Common Protocol for implementing Various DHT Algorithms".
29. Quora, "Which is the most popular routing technique," Retreived from http://www.quora.com/Which-is-the-most-popular-routing-technique-for-distributed-hash-tables [Accessed 7/1/15]
30. A. Rowstron and P. Druschel, "Storage management and caching in PAST, a large-scale,persistent peer-to-peer storage utility" in Proc. ACM SOSP'01, Banff, Canada, Oct. 2001.
31. A. Rowstron, A.-M. Kermarrec, P. Druschel, and M. Castro, "Scribe: The design of a large-scale event notification infrastructure". June 2001.

AUTHOR(S) PROFILE

Jyoti Chaudhary, is Pursuing post-graduation in M.Tech, Computer Science at DIT University, Dehradun.

Dr. Rama Sushil, received P.hd degree from IIT roorkee in Computer Science and Hirosaki University Japan, provided her one year research fellowship for research work in informatics Dept. She is now Head of the Dept. of Information Technology at DIT University, Dehradun.

