Automatic Cloud-based Digital Forensics Artifacts Categorization

Shabnam Mohamed Aslam

Department of Information Technology, College of Computer and Information Sciences,
Majmaah University,Al Majmaah, 11952, s.aslam@mu.edu.sa@mu.edu.sa

Abstract

Cloud Computing technology enables to delivery of online services on-demand to clients. The boom of cloud computing reaches its peak and now available services from different aspects right from education to entertainment. The world top organizations run with the base of cloud services. On the other side, there is a drastic growth in cybercrimes. The top-notch technology called Digital Forensics emerges to control the Cybercrimes in part. This research focuses on performing digital forensics process on cloud computing in such a way that prevent security breaches through cloud services and trace the incidents and forgeries. It is explored some ways in which the digital artefacts can be collected from cloud services that are widely being used by every other corner of the world in this paper. The ways to retrieve forensic evidentiary artefacts from the cloud services are engineered using digital forensic tools. Pilot tests are conducted to analyse the success of artefacts retrieval from current cloud SaaS.

Keywords:

Cloud Forensics; Digital Forensics; Cloud Cyber Security; Cloud Computing

1.Introduction

The utilization of distributed computing has expected advantages to companies, including expanded adaptability and effectiveness. The virtual applications deliver more elasticity over an in-house physical IT framework since the applications [1] can be vastly reconstructed or squamous to map with the latest and emerging requirements deprived of the necessity to acquire the newest and possibly respective hardware. Correlative to this, the utilization of distributed computing can decrease the expenses of giving IT administrations, by taking out excess registering force and capacity, lessening support necessities and diminishing fixed capital responsibilities. The research studies reveal that there is 37% of cost savings have been obtained by organizations who migrate the IT infrastructure from the datacenters to Amazon Cloud. Digital forensics in distributed computing is another discipline identified with the expanding utilization of PCs, organizations and computerized stockpiling gadgets in various crimes in both conventional and High Tech. Then, cloud computing seems to be an existing research issue to digital investigations, it is very important to understand the effect that pertains to cloud by forensic processes and what way the old techniques, application controls and techniques might adapt to cloud environments. As an outcome, the existence of the boom of cloud forensics in its infancy, an emergency is raised to sort out the digital investigation with the use of some tools and techniques in the cloud platform. With the motivation of understanding the opportunities and limitations of conventional digital forensics methods deployed to the distributed computing termed Cloud, it has been performed a research study based on a set of popular SaaS cloud applications, to see if captured IP packets and traces are available in the local machine, extracted with openly available forensic tools, are enough to take legal action against the culprit in court [2]. I rejected ahead of time the choice of making a solicitation to hold onto a cloud server in the unfamiliar locale as it is a tedious action, with restricted added esteem from a specialized stance.

1.1. Technical Background

For enterprises, Digital Forensics is an important part of the Incident Response process. Forensic Investigators determine and log facts of a criminal incident aided to be the evidence to be used for law enforcement. A digital investigator is a person who desires to follow the proof and prove the crime. Consider a security vulnerability [3] that exist at an enterprise, ends with data steal. In the present circumstance, a computer forensic analyst would enter and identify what way the hackers escalate the privileges of the target network to penetrate the network. Moreover, it is being analyzed that they are the steps the hacker go across the network scanning, any malware has been installed or hooked to the operating system and so on. The role of the digital forensic investigator is to recover deleted documents, artefacts that are susceptible to the criminal incident occurrence from computer data storage devices such as zip and USB drives and diskettes, with erased, harmed, or handled in any different type of manipulation on the data. The meaning of the phrase cloud forensics is defined as an inter-disciplinary between cloud computing and digital forensics [8]. Cloud forensics is the composition of the multifaceted system to serve organizational, legal and technical implications. There are a set of tools and techniques are used from a technical perspective to perform forensic processes in cloud computing environments. The design structure for internal staffing, producer-consumer relationship and external assistance fulfilling the specific incident response roles are termed as organizational perspectives. The legal perspective activities of digital forensics include the agreements and regulations defined for carryout the forensic process to be secured and will not breach any laws or regulations under any jurisdictions where the data is stored, throughout the investigation [5]. Broad network access, rapid scalability, metered services, on-demand self-service and resource pooling are the fundamental characteristics of cloud computing. Cloud design depends fundamentally on three centre advancements: web applications and web administrations, virtualization, and cryptography. As per the previously mentioned NIST definition [2], administrations in the cloud are given by the accompanying essential models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Specifically, with IaaS an entire operating system, services, and stored information are remotely available to the client whereas, with PaaS, clients are assigned the plugins to build and host internet services on a user computer, and with SaaS key applications and data based on a remote machine are made available on-demand to users [6,7]. According to the National Institute of Standards and Technology, the cloud models are classified into four elements. They are Public, Private, Hybrid and Community cloud [2]. The resources are pooled, applications and services are available on-demand regardless of the type of devices on the cloud. The impact of on-demand availability encourages the users to make use of mobile phones and other digital gadgets to avail cloud services at any time.

Fig. 1. Cloud forensics workflow

1.2. Paper Outline

The overview of the following section of the paper is as follows: Section-2 mention the threats of cloud computing in Section-3 and describe the outline of the conducted research study and in Section-4 discuss the relevant results. I finally conclude our research in Section 5.

2.Cloud Computing essentials

There is consistently a danger that client information can be gotten to by others. So it is important to maintain storage protection and cloud protection as data confidentiality relies on cloud protection. The web is the best way to distribute computing. When there is no web association in your place, or the web way to the cloud supplier is in a difficult situation, consequently, admittance to your distributed computing machine will be separated. Presently this is the place where the greatest snag is occurring in agricultural nations and distant regions that don't have great web access. The public cloud is the server where if it expands to danger, the server will down. Security and privacy are the most doubtful things in cloud computing [4,5]. The practical usage of a cloud computing system assures the security and confidentiality of data for the consumers so that becomes a trusted server. The clients cannot face the server legally when it performs insecure resulting in the error in data. Cloud computing is receiving queries to solve by computing in online, hence there is more exposure to data security attacks by the attackers hence the data privacy is not assured. Cloud Computing is vulnerable to data privacy and security as it is online. The aspect of the data is being shared online employing Data mobility characteristics, the user knows to retrieve data from the cloud if at all the server is down for one day. Cloud Computing is enabled with customer service 24/7 which provides data availability in the form of maintaining temporary data storage service and serving from that whenever the server is down. The degree of excellence of cloud computing servers is a notorious account to decide to provide cloud computing server service, providers. When the server is down or the performance is not good, the users get affected poorly as the server quality is not good. These aspects are called the pros and cons of Cloud Computing services. Predominantly I cannot say that Cloud is always good. From the study, it is understood that there is no privacy for data as the data is stored in different places of the cloud, but also at the same time, it shares the resources efficiently and is also being scanned for virus attacks periodically. At another end, the client devices use the IaaS, PaaS and SaaS service models where the evidence can be extracted for cloud forensics. The only source from which data can be collected related to cloud computing in the user device is SaaS applications installed in client computers. This is the reason for conducting an exhaustive forensic investigation in the client computer to collect evidentiary materials. [7].

3.Client Evidence Analysis

I made a pilot study of cloud forensics where the tests are planned on SaaS applications to prove that, searching PC artefacts, it is possible to identify specific evidentiary material about the user-computer communication. Based on this, I have identified and reviewed document editing and photo sharing SaaS plugins, such as Google Drive [11], Central Desktop and Cintas [12], to demonstrate that potential evidence may be found in file systems and registry, SQLite databases, web browsing history, downloads and cookies of the Web browsers. I also analyzed Dropbox, a familiar file sharing SaaS application that may work both as a net via cloud service, as Google Document. The service of Google Drive is providing platforms for users can edit the document with the sword in their browser and can be stored in local machine as well as in the cloud on their account. They could then download it as an Office consistent record, or offer it with other Google clients, who could be allowed to see just or to alter. At the point when different clients saw it all the while, with altering consents, they could at the same time see each other's cursors, and type in the report. Google Drive gulped this, developing the file system and altering abilities. Desktop Central followed Google Drive by additional characterizing what was going on with record the document accounting. This framework is intended for a wide cluster of expert purposes including accounting, teaching-learning, finance, law, corporate and pretty much whatever else that is for the most part standard. It utilizes SQL and is adaptable enough for a wide scope of business extensions and business growth, and has the most extreme security. It's somewhat costly at $90/month, however, it's justified for the appropriate association, sharing, altering and dispersion of significant convention archives and business information. Cintas is a multi-administration proficient organization giving human resources, accounting, and presently managing official documents through SaaS stages. This is like Desktop Central, however offers the increased of a ton more languages, and a few formats and conventions for additional archive types, similar to land management and clinical management industries. Along these lines, I see that SaaS manage the executives advanced from a common document framework and altering limit in a lovely crude structure, to a refined, task-situated kind of programming, which exceptionally experienced proficient organizations then, at that point, proceeded to refine further, into an extremely standard and generally grew new programming industry. Consider the SaaS video editing applications such as InVideo[14], VSDC, Filmora [13]. InVideo makes drawing in content and makes it appropriate marking with the utilization of the most recent video altering programming. As fledglings might not have a specialist hand at altering yet, the in-assembled layouts in InVideo can be useful. It helps make an expert looking video with the best utilization of plan and components accessible on the product. In digital forensics, video type is investigated to know whether illegally produced? This examination likewise leads video source ID and video steganography investigation to uncover stowed away data. In particular, the video source ID is a significant proof source to distinguish the sources [8]. Filmora application performs video editing simplified tasks. It is an amazing asset choice to give shape to your imaginative thoughts and works out positively for all video makers. The features can help work on audio effects, cut background noise, and effects to video. Related to the evidence collection from the cloud, I doctored five pilot tests plans, numbered from 1 to 5, where the basic steps are establishing a manifest with the cloud service and creating a user account. In each scenario, I performed the tests listed below, each labelled with a unique sequence number and a description of the performed action.

Test Plan 1: Google drive accessed via a web browser
1.1: Logging to www.drive.google.com
1.2: Upload folder of files
1.3: Update the documents
1.4: Delete the folder

Test Plan 2: Desktop Central access through web
2.1: Software installation
2.2: Manage patches
2.3: User logging
2.4: Project creation
2.5: Create document using template

Test plan 3: Cintas access through a Web browser
3.1: Software installation
3.2: Manage patches
3.3: User Logging
3.4: Project creation
3.5: Create a management document using a template

Test plan 4: Access shutter stock using a web browser
4.1 Logging to www.shutterstock.com
4.2 Upload picture
4.3 Download picture
4.4. Keyword search of a picture

Test plan 5: Access Grammarly from a web browser
5.1 Logging www.Grammarly.com
5.2 Upload word document file
5.3 Check grammar in word document
5.4 Save corrected word document to Grammarly local folder

4. Pilot test result study and discussions

The author tested the cloud services against the most widely used web browsers (i.e. Mozilla Firefox, Google Chrome and MS Internet Explorer) through the test plans from one to five on the client-side. I collected the evidence of interaction between the local computer and the cloud as such the browser cookies, cache and history information of the browser and network traffic using digital forensic tools and packet sniffer tools. According to test plans two and three, a set of traditional forensics tools is used to validate the plugins installed by Desktop Central the cloud application version is known as iMeetCentral and Cintas project management Saas software. The SaaS names Central Desktop, Cintas and iMeet Central are refer to the same cloud application. Hence the terms are used at different places of the document denotes the same cloud application. The evidentiary files are analyzed to view the meta information of the file such as file creation time, last access time and file size. The pilot tests are performed 3 to four times each, the former using live forensics tools on a powered-on laptop computer running Windows 10 Home Edition 64 bit and the latter with post mortem forensics tools on a physical image of its hard disk and with FRED system. The following web browser versions are used to test Google Drive, Grammarly and Shutter Stock.

1.Google Chrome 9.7
2.MS Internet Explorer 5.5
3.Mozilla Firefox

As well as the tested against the following openly available Nirsoft live forensics tools [9], on the powered-on system. The forensic tools used in this research are license free tools available in online. This section describes the results obtained after analysis of pieces of evidence collected from the cloud from the pilot tests from 1 to 5.

4.1Test Plan 1- Google Drive accessed via the Web browser

It has been viewed the history, cache and cookies of IE, Google Chrome and Mozilla Firefox using forensic tools such as IECookiesView, IEHistoryView, MozillaCacheView, MozillaCookiesView and MozillaHistoryView after the test one. The history information states that Drive. Google login page is present in the access list of the history of the browser. The traces of folder creation in Google drive is present in the cookies of the browser. The copy of the files created is present in the cache as shown in figure 1. The Wireshark packet sniffer is used to scan the traffic where it returns that Google drive uses SSL transmission which is a secured mode for eavesdrop by viewing the TCP port 443 is open in the target server. The ChromeCacheView shows secure file upload as stated in figure 6 the. column server-response has the value “HTTP” which is secure communication.

Test Plan 2- Desktop Central access through the web browser

The windows registry is explored using regscanner and Regedit forensic tools and found that the product id entry was added for the newly created IT management application named Desktop Central cloud service that is shown in figure 4. The Wireshark packet sniffer is used to scan the traffic where it returns that Desktop Central uses SSL transmission which is a secured mode for eavesdrop by viewing the TCP port 443 is open in the target server which is shown in figure 2. Also as specified by the screen of Chromecookies-View captured in figure 5, Central Desktop cloud service uses unsecured communications, the secure column shows "No" value for all the Central.com urls.

4.2Test Plan 3- Cintas SaaS project management software accessible through the web browser

The windows registry is explored using regscanner and Regedit forensic tools and found that the product id entry was added for the newly created project management service by Cintas cloud service. The Zenmap packet sniffer is used to scan the traffic where it returns that Cintas [10] uses SSL transmission which is a secured mode for eavesdrop by viewing the TCP port 443 is open in the target server as shown in figure 2. But it has been identified as the server is Heartbleed vulnerable means anyone can access the server remotely.

4.3Test Plan 4- Access Shutter Stock using the web browser

The forensic tools IE history view, ChromehistoryView and Mozilla history view shows that there is a trace of files downloaded from Shutter Stock and trace of login page access was present, the meta-information of the files has been expanded using Sleuthkit. The picture files were found to be legal files as it shows the owner of the files is authorized. The file sizes are matching with exact file size whatever folder explorer shows and the Sleuthkit result shows. The browser CacheView extracts the copy of the uploaded picture file and downloaded picture files.

4.4Test Plan 5- access of Grammarly service by the web browser

The forensic tools such as reg edit, registry viewer are used to view the registration information after test five is completed. There is a trace of a new product ID in the registry for installation of Grammarly service in the local disk. The cloud server communication is scanned and identified TCP port 443 is open which uses SSL transmission to ensure data security. The document file uploaded to the cloud is secured against eavesdrop is ensured

Figure 1 Chrome cache view artifacts

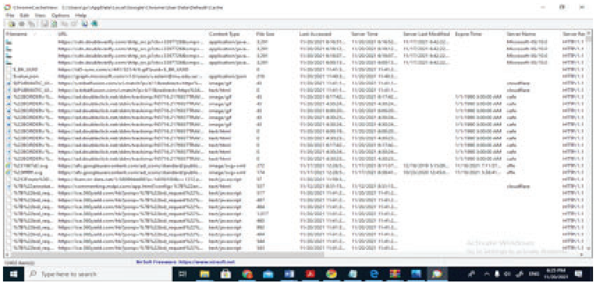


Figure 2 Wireshark artifacts

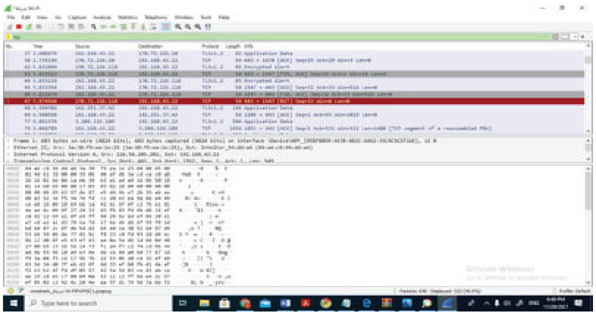


Figure 3 Wireshark artifacts for iMeet Central

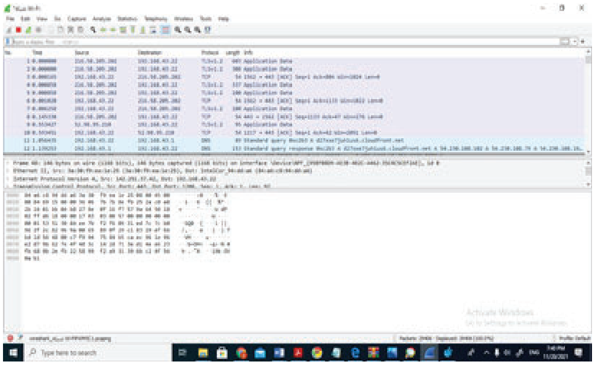


Figure 4 Regedit Web client entry (iMeet Central) artifacts

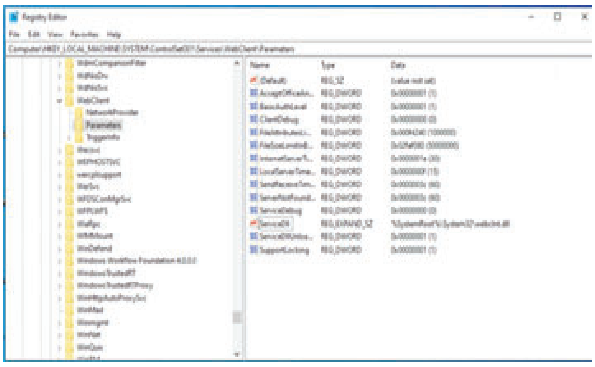


Figure 5 Chromecookiesview Central desk artifacts

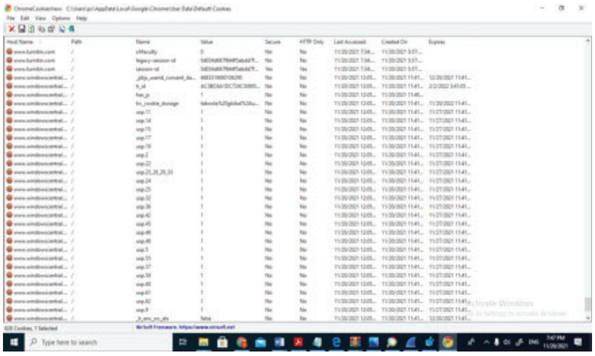
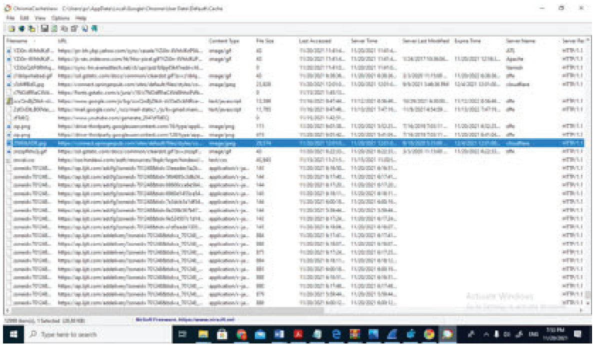


Figure 6 ChromeCacheview- Google Drive file download artifacts



5 Conclusion

In this research, Could Computing threats against the security breaches are discussed, the role of Digital forensics in cloud computing is emphasized. Cloud forensics and its challenges are addressed partly by utilizing digital forensics tools. The research question "What and how the cloud artefacts can be collected as evidentiary artefacts to test against digital crime?" is answered through five pilot tests result and discussion. It has been utilized digital forensic tools such as browser component viewers, Banner Grabbing using WireShark and Zenmap tool to identify Eavesdrop of communication between the local machine and cloud server. This research is a way to explore the new ways of collecting cloud artefacts using conventional digital forensic tools and in future, the challenges of digital forensics in the cloud using Network devices and Mobile devices will be analyzed.

Conflict of Interest

The author has no conflict of interest.

Acknowledgements

The author would like to thank the Deanship of College of Computer and Information Sciences and Deanship of Research Majmaah University for supporting the research.

References

[1]Devi SK, Govindarajan S, Maheswari KU. Hgrid: An Economical Model for Mass-Health Care System Using Latest Technology (Grid Computing).

SRM MANAGEMENT DIGEST-2011. 2011:426

[2]Marturana F, Me G, Tacconi S. A case study on digital forensics in the cloud. In2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery 2012 Oct 10 (pp. 111-116). IEEE.

[3]D. Birk. Technical Challenged of Forensic Investigations in cloud computing environments. 2011. Retrieved May 10, 2012, from http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf.

[4]D. Barrett. Virtualization and forensics a digital forensic investigator's guide to virtual environments. Syngress Publishing, 2010.

[5]F. Marturana, R. Bertè, G. Me, S. Tacconi. Mobile Forensics "triaging": new directions for methodology. In Proceedings of VIII Conference of the Italian Chapter of AIS (ITAIS 2011) Rome, Italy, Springer, 2011.

[6]F. Marturana, R. Bertè, G. Me, S. Tacconi. A quantitative approach to Triaging in Mobile Forensics. In Proceedings of International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, (TRUSTCOM 2011) Changsha, China, pages 582-588, 2011.

[7]F. Marturana, R. Bertè, G. Me, S. Tacconi. Data mining based crime-dependent triage in digital forensics analysis. In Proceedings of 2012 International Conference on Affective Computing and Intelligent Interaction (ICACII 2012) and IERI Lecture Notes in Information Technology, 2012, in press.

[8]F. Marturana, R. Bertè, G. Me, S. Tacconi. Triage-based automated analysis of evidence in court cases of copyright infringement. In Proceedings of First IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012), in conjunction with IEEE ICC, Ottawa, Canada, 2012, in press.

[9]K. Ruan, J. Carthy, T. Kechadi, M. Crosbie. Cloud forensics: An overview. In proceedings of 7th IFIP International Conference on digital forensics, Advances in digital forensics, Vol. 7, Springer, 2011.

[10]Xiao J, Li S, Xu Q. Video-based evidence analysis and extraction in digital forensic investigation. IEEE Access. 2019 Apr 26;7:55432-42.

[11]Quick, D. and Choo, K.K.R., 2014. Google Drive: Forensic analysis of data remnants. Journal of Network and Computer Applications, 40, pp.179-193.

[12]Escriva, D.M.L., Torres-Sospedra, J. and Berlanga-Llavori, R., 2018. Smart outdoor light desktop central management system. IEEE Intelligent Transportation Systems Magazine, 10(2), pp.58-68.

[13]Natasha, D., Nopita, D. and Elfiza, R., 2020. THE EFFECT OF FILMORA ON STUDENTS'MOTIVATION IN WRITING AT SEVENTH GRADE OF MTSN TANJUNGPINANG. Student Online Journal (SOJ) UMRAH-Keguruan dan Ilmu Pendidikan, 1(1), pp.290-298.

[14]https://make.invideo.io/online-video-maker