KF7000

Cloud Application Forensics

Shona Start
w17019752

Contents

Introduction

This paper will analyse and discuss forensics investigations in cloud applications. It will discuss the processes and techniques that can be used in both client-side and provider-side investigations. In the first half of this paper I will define cloud applications and important technical details that can impact an investigation, such as the service and deployment models. In the second half I will analyse how computer forensics is applied to cloud applications and the processes, techniques and difficulties an investigator may encounter during a cloud investigation; with a focus on the identification, preservation, collection and analysis phases.

What are cloud applications

While cloud computing has been around since the 1990s, it did not reach mainstream use until the mid-2000s. Since then it has been growing with increasing applications using cloud computing. Gartner, a global research and advisory firm, predicts that throughout 2022 "*the market size and growth of the cloud services industry* (will be) *at nearly three times the growth of overall IT services.*" (Gartner, 2019). Although part of this growth will be because of Internet of Things (IoT) systems that make use of the cloud, the use of cloud applications will also expand.

A cloud computing application is an internet based program where at least some of the processing logic and data storage in done in the cloud. Clients of cloud applications often interact with these services via web browsers and Application Programming Interfaces (APIs). The National Institute of Standards and Technology (NIST) define Cloud Computing as:

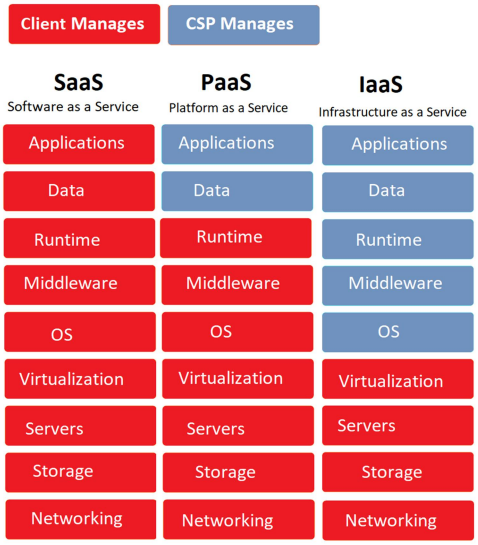
"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." (National Institute of Standards and Technology, 2011).

Essential Characteristics

As stated in this quote cloud computing has five essential characteristics. These are:

- On-demand self-service: A client can provision computing capabilities as required without needing human interaction with service providers.
- Broad network access: Computing capabilities are accessible all over a network and can be accessed through standard mechanisms (Mobile Phones, Laptops, Desktops etc.).
- Resource pooling: The computing resources are combined to serve multiple clients using a multi-tenant model. Resources are dynamically assigned/reassigned depending on consumer demand.
- Rapid elasticity: Computing capabilities can be elastically provided/removed to scale with demand.
- Measured service: Resource usage can be monitored, controlled, and reported to providing transparency for both provider and client (National Institute of Standards and Technology, 2011).

Service Models



Cloud computing is provided in three main service models; these are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Each model is designed to resolve different requirements.

The SaaS model allows a client to use applications from a provider without having to install and run the cloud infrastructure on their own system. Instead an application service provider hosts the applications and makes them available to clients; usually over the Internet (UK Parliament, 2020. Diaby T and Bashari Rad B, 2017). This is the most predominant model and is used by many common applications including Google Applications, Amazon, Slack, Dropbox and Microsoft Office (Vladimirskiy V, 2016). Clients of the SaaS model typically do not know or have any say in the physical location of their data. Many cloud applications even purposely hide the location of data from clients so that data can be moved or replicated without the clients knowledge. This can create difficulties in accessing data required for a forensic investigation (Ruan K et al, 2011).

On the other hand, the PaaS model provides clients with a platform where they can develop and host their own software and applications. The provider will often give access to programming languages, libraries, services, and tools. This model is often used by application developers, similar to the SaaS model this model can restrict the access to data and the cloud platform which can create difficulties in accessing data required for a forensic investigation. (UK Parliament, 2020. National Institute of Standards and Technology, 2011. Grispos G, Storer T and Glisson W.B, 2012). Examples of PaaS applications include Windows Azure, Google App Engine, Apache Stratos and OpenShift (Watts S and Raza M, 2020).

When using the IaaS model, the provider maintains all the hardware and computing resources and allows the client remote access. The client can deploy and control operating systems, applications and other software in the cloud as a virtual machine (VM) but cannot control the cloud infrastructure (UK Parliament, 2020. National Institute of Standards and Technology, 2011). This model is considered easier when it comes to gaining access to data required for a forensic investigation, compared to the other service models; because the client has access to the most data on an IaaS model. However, the data on an IaaS is often more volatile as this type of model uses a large amount of dynamic scaling. This can increase the likelihood of data becoming lost (Ruan K et al, 2011. Grispos G, Storer T and Glisson W.B, 2012). Examples of IaaS include Amazon Web Services, Windows Azure, Cisco Metacloud, and Google Compute Engine (Watts S and Raza M, 2020).

Deployment Models

The four deployment models for cloud forensics are private cloud, community cloud, public cloud and hybrid cloud.

In a private model, the cloud infrastructure is used exclusively by a single organization and their clients. Private clouds are often classed as the most secure clouds, as these are not accessible by the public. This infrastructure could be owned and operated by the organization or by a third-party

provider. It could also exist on or off the premises of the owning organization (National Institute of Standards and Technology, 2011. Diaby T and Bashari Rad B, 2017).

Community clouds are like private clouds; however, they are shared between multiple organizations. As with private clouds could be owned and operated by the one or more of the organizations or by a third-party provider and could exist on or off the premises of the owning organization. This type of cloud deployment is often used to reduce the cost of cloud apps. (National Institute of Standards and Technology, 2011)

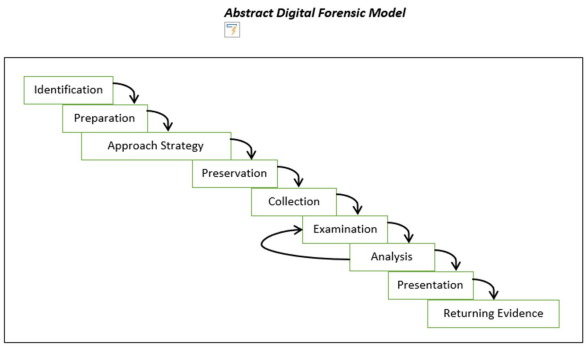
The public cloud deployment model is one of the most popular types. It is predicted that in 2025, 49% of the world's data will be stored in public clouds (UK Parliament, 2020). Public clouds are accessible by the public and often use a pay-as-you-go service by a provider organization. This organization owns, maintains and manages all cloud infrastructure, and will store everything on their own premises. It is almost guaranteed that a public cloud will contain data from more than one user with larger companies providing the infrastructure for millions of clients (Grispos G, Storer T and Glisson W.B, 2012. National Institute of Standards and Technology, 2011).

A hybrid cloud model is a combination of multiple deployment models that remain separate but share resources, often for load balancing purposes. As they are a combination; hybrid clouds can be owned and operated by an organization or by a third-party provider and can exist on or off the premises of the owning organization (National Institute of Standards and Technology, 2011).

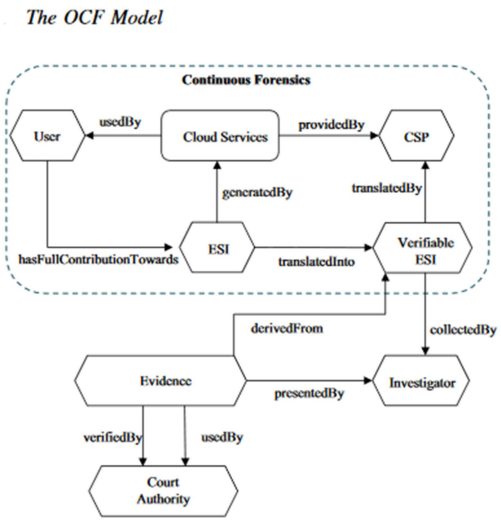
Applying computer forensic to cloud applications

Forensic Models

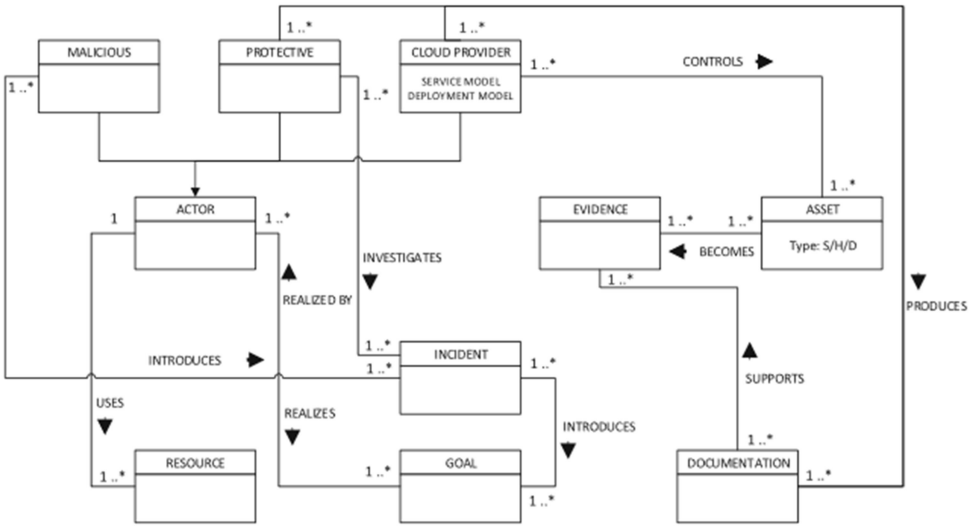
Digital forensics models are the process used to conduct forensic investigations. There are many types of models to fit different investigations but most of these share the same traits. More generic modules such as the Abstract Digital Forensics Model (ADFM) can be applied to a large range of investigations and technologies including cloud applications. However, specified models designed with cloud forensics in mind do exist.



One example is the Open Cloud Forensics (OCF) model. This model uses a continuous process flow. It considers all the entities the investigator will have to interact with in this type of investigation including outlining the role of cloud provider (Zawoad, S et al. 2015).



Another example is the Meta-model. This model takes into consideration the actors, assets, resources, evidence and documentation needed in a cloud invitation (Simou, S et al. 2015).



Meta-model for assisting a cloud forensics process

Identification

The method for identifying if a potential criminal has taken place will depend on both the service and deployment model the cloud application is using. On cloud applications, using the SaaS and PaaS model there is no easy way of identifying evidence on the server side. Whereas, in an IaaS there is more of a potential to identify evidence as the client will have access to some cloud infrastructure (O'Shaughnessy S and Keane A, 2013).

On the server-side, a traditional way of identifying malicious activity is with Intrusion Detection Systems (IDS). IDS's are devices or software that are designed to monitor a system or network in order to detect malicious activities and often have features like firewalls, anti-virus, logging tools and scanning tools. There are multiple types of IDS's, the main two being Network based IDS; which monitor network traffic, and Host based IDS; which monitor operating system files. Both of these can be used on a cloud system. However, IDS's should not be relied upon entirely, as all types need an up-to-date library of threats, so that newer threats can be detected. Even then, an IDS cannot detect all types of malicious activities. Another issue with relying on IDS's is that it is the providers (SaaS or PaaS) or clients (IaaS) choice whether to use an IDS, so an investigator cannot rely on one being present (Kene S.G and Theng D.P, 2015).

Identifying evidence on the client-side involves finding the application or web browser the client uses to access the cloud. In clouds using the SaaS and PaaS models most cases with data relating to cloud apps will be encrypted on the client-side, limiting identification. But this does not mean nothing can be found, especially in log files created by the application (Simou S et al. 2016).

Another traditional way of identification used by forensics investigators is log files. Log files are an extremely important asset in computer forensics as they can provide a record of events for software, systems and networks. Often access to log files is the top priority in an investigation, sometimes compared to "eyewitnesses" of the crime. However, collecting logs from the server-side can be difficult especially when multiple users share the same processing and network resources. Many

providers will not provide access to application or system or network log files. And even if they do in clouds using the PaaS or SaaS models, most system log files will not provide data of use on clients. In these modules, clients cannot access systems, only interfaces. Server-side logs are also controlled entirely by the provider, which means they may not choose to archive logs, care about the volatility of their logs or even store logs spread across multiple servers (Simou S et al. 2016, O'Shaughnessy S and Keane A, 2013). There are proposed solutions for these problems. For example, Zawoad et al. suggests a secure-logging-as-a-service (SecLaas) tool designed to allow providers to store logs from a IaaS model in a manner that enables forensic investigators access, while preserving confidentiality for clients (Zawoad S, Dutta A.K and Hasan R, 2013). However, this solution and many others are reliant on providers cooperation to implement such mechanisms to their systems.

One of the major challenges with server-side identification (and cloud forensics as a whole) is its dependence on the provider. Providers are responsible for assisting investigators, especially in SaaS and PaaS. However, in some cases, providers are not willing to provide access to information or systems. A provider may choose to identify, preserve, and collect evidence itself, but this leads to integrity issues as it will be unlikely this will be done by a certified forensic practitioner. Further complications can occur in a community cloud or private cloud using third parties as the investigation will have to cover all parties involved (Simou S et al. 2016). One mechanism that could assist in this is the service level agreement (SLA). The SLA is a contractual document that defines the terms of use between the provider and the clients. SLAs should contain clear details on how forensic investigations will be handled by the provider and client, however this is not always the case as guidelines concerning forensic investigations are often left out. SLA standardization and international regulation is likely needed in order to allow investigators to access the data they need as well as preserve the rights of providers and clients. (Alenezi A, Atlam H.F and Wills G.B, 2019)

Preservation and Collection

One of the most important factors in proving preservation of data is the chain of custody. The chain of custody should provide a history of the handling of all evidence during an investigation and is required for items/data to be legally considered as evidence in court. Creating a chain of custody for the client-side usually just requires following normal computer forensics guidelines. However, creating a chain of custody for a server-side cloud investigation can be challenging, as investigators often have to rely on the provider to create forensic imaging of evidence while still providing details on how and where the evidence was collected, how it was stored, and who accessed it (Ruan K et al 2011, O'Shaughnessy S and Keane A, 2013).

Forensic imaging is when an exact copy of a piece of digital evidence is taken for analysis. This is done to prevent loss of data and provide validity. There are multiple sources of digital evidence that can be taken from a computer, including the hard drive, volatile memory and network traffic. However, if an investigator is intending to collect from multiple sources, they need to do this in order of volatility. The most volatile is network traffic, as this data is immediately lost unless it is collected. In most cases, a live acquisition would be needed to collect network traffic but performing a live acquisition can modify the next most volatile source, volatile memory. Volatile memory can be altered whenever an action is taken on a computer and is continuously overwritten during normal use. This data is also completely lost when a machine is powered down. The least volatile source is the physical data stored on a hard-drive or similar devices.

Collecting a forensic image of a client-side device would typically be performed by physically connecting the device to the investigators computer which will contain the imaging software used. If

physical access of the client-side device is not possible, then collecting an image of this device is impossible (Grispos G, Storer T and Glisson W.B, 2012). If a forensics image is taken the usefulness of this will be determined by the service model used. The IaaS will provide the most amount of useful data, if an image of the VM can be taken. However, in PaaS the only information on the client-side will be specific application data and in SaaS, even less data will be stored. In these cases, it will be vital that the investigator works with the provider, as this is where they will have to retrieve the data (Simou S et al. 2016).

The UK Investigatory Powers Act 2016 states that communications service providers must store user connection records for up to a year, and that national security services can send a data retention notice to any provider in order to requests access to communications data about clients. The act also allows for "technical capability notices" which in some cases may mean providers have to remove electronic protection such as encryption from communication and data (UK Parliament, 2020. UK Legislation, 2016). However, even with this law, performing forensic imaging on the server-side can be extremely difficult.

One of the main reasons for this is because the data will often need to be stored on multiple physical devices, which in some cases can reside in different geographical locations. This creates multi-jurisdiction issues which can make an investigation very difficult, sometimes impossible, especially when laws and regulations regarding confidentiality and privacy differ between countries. Seizing hardware when it is situated in another country is almost always impossible leaving the only solution to rely on local law enforcement to create an image. This is usually only possible if treaties are established between these countries (O'Shaughnessy S and Keane A, 2013). For example, in the United States (U.S) a law exist called the US CLOUD Act. This law allows law enforcement agencies to request data from U.S internet service providers even if the data is stored in another country. As part of this act, the UK and US are under an agreement that they may each request data from providers located in the other country, if the requesting nation has jurisdiction over the provider. This means that if a provider based in the UK stores data in the U.S, national security services can still request that data (UK Parliament, 2020. 115th Congress, 2018).

Another major hurdle is because many IaaS and PaaS clouds store client data in the same environment. This resource-sharing can mean that providers are unwilling to give access, as it would be a breach of confidentiality agreements. Investigators need to maintain confidentiality and privacy while also ensuring only data relating to the particular client is gathered (Pichan A et al. 2015).

Analysis

The amount of data stored by providers can be enormous, which can make it extremely difficult to search for evidence. This is especially true in SaaS and PaaS clouds, as these can have systems that contain many different applications. Data mining can be used on the cloud to streamline the analysis of large amounts of data. This involves using software to look for patterns in data, however, the forensic implementation of this on the cloud needs more investigations before it will be usable. Another suggestion is data reduction techniques, for example selective imaging of the files and data of high forensic value. Of course, with this method there is a higher change of evidence being missed so it should never be used as a replacement for full forensics analysis (Quick D and Choo KK, 2016, Grispos G, Storer T and Glisson W.B, 2012)

Recovering deleted data is an important step when analysing digital data. In a regular investigation, deleted data can normally be recovered using data carving techniques, however, in the cloud this is

a lot harder to do. In some cases, it is possible to collect deleted data from the cloud, but only if the data is not overwritten; this is a slim chance with the volatility of cloud data. This is further complicated by the fact that in many cloud apps, all it takes is a client cancelling their account for all their data to be wiped by the provider and in a shared cloud it is likely that the space an old clients data was in will be allocated to a new client, creating confidentiality issues (Pichan A et al. 2015). Following the European Parliaments (EP) Data Retention Directive, public communication providers must at least keep some information about past and present users, including data necessary to identify the source, destination, date, time, duration and type of communication as well as the clients communication equipment and the location of mobile equipment (European Parliament 2006).

During the analysis it is important to reconstruct the crime scene. This involves organizing the analysis results from the physical and digital data, to establish the facts for the incident. Reconstruction in the cloud is a challenge as tools and guild lines for this are limited. There are, of course, further difficulties with this if the provider has not released all the data (Pichan A et al. 2015). One way of reconstruction is to establish a time line of events. During an investigation, establishing a timeline of events helps to build a picture of all the events happening on a device or set of devices during that time frame. Often, reconstruction of the sequence of events is easier as most actions performed on a digital device are time stamped automatically. However, an investigator will need to be aware that data from different geographic locations may use different time zones, and therefore different timestamps. Models have been proposed to assist in collecting from the cloud. For example, Secure-Logging-as-a-Service (SecLaaS), which is a model for collecting any type of log files from any source or location; including servers, applications and devices (Zawoad S, Dutta A.K and Hasan R, 2013, O'Shaughnessy S and Keane A, 2013).

The evidence collected during analysis must be validated to ensure it is legally acceptable. This involves ensuring all data, applications, and results be proven as valid. The validation of data is often done by comparing the data to previous versions or supplementary sources. Software hashing tools are also used; they create a 'signature' for every file on a system, this 'signature' will change if the file is altered in anyway. This method can be used with data collected from cloud applications and some services, such as Amazon Web Services, provide hashing mechanisms of their own (Roussev, V, 2009. AWS, 2019).

Forensics Tools

Preservation, collection and analysis of cloud applications require forensics tools, however, there is a lack of appropriate and reliable cloud specific tools. Currently existing forensics tools are often used to analyse data from the cloud, but software has not always been tested for cloud data. Examples of cloud forensics toolkits include:

Cellebrite UFED Cloud Analyzer: This is software designed for preservation and analysis of client-side cloud application data, including data from social-media and cloud storage apps. It can even provide access to private user cloud data. However, this software is only designed for iOS and Android mobile devices so is unusable when collecting from a computer (Naaz S and Siddiqui F, 2016. Beet N, 2016)

Forensics Open-Stack Tools (FROST): This toolkit is designed for use in client-side investigations involving the IaaS platform OpenStack; one of the biggest IaaS platforms. This software does not interact with the system, instead it uses the management plane. This means to gather most data no

interaction is needed with the provider, only with the client. This is of course an extremely useful toolkit for OpenStack but is only possible with cooperation from the provider to create this type of toolkit (Dykstra J and Sherman A, 2013. Digital Forensics vs. OpenStack, 2016).

Elcomsoft Cloud eXplorer: This software is designed for collecting data from Google accounts. It gives access to cloud data stored in apps such as Google Drive, Gmail and Google Chrome. In some cases it even allows for authentication of an account without a password and bypassing of two-factor authentication (ElcomSoft Co.Ltd, 2019).

F-Response Universal: This is a server-based remote access software used for live forensics. It provides cloud collection features for many cloud applications including Dropbox, Gmail, Google Drive, Microsoft Office, OneDrive and Amazon S3 (F-Response, 2017).

Conclusion

There are always challenges with conducting a forensic investigation involving the cloud, no matter which combination of service and deployment models are used. One of the biggest issues is access to the cloud and dependence on the provider to do so. This is because if an investigator can't even access the data, they have no hope of performing any sort of preservation or analysis. Most solutions are dependent on the trust of the provider, such as allowing them to make a copy of their data to hand over to law enforcement. Understandably, providers need to protect themselves and their clients, but this provides issues for the chain of dependency and could make evidence unreliable. The volatility of the cloud complicates this issue further, as this means data can easily be lost if forensic standards are not performed correctly. One of the biggest reasons for the issues in the cloud is the lack of legislation and guidance. But even when legislation is in place, the global aspect of the cloud means that no progress can be made without further legislation between countries. Many of the solutions to problems discussed in the paper cannot be fully relied upon as they have too many flaws. More research and cooperation is needed between law enforcement and providers if solid investigations are to be possible in the future.

References

115th Congress (2018). H.R.4943 - CLOUD Act. Congress.gov Available at: https://www.congress.gov/bill/115th-congress/house-bill/4943/text [Accessed December 2020]

Alenezi A, Atlam H.F and Wills G.B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. Journal of Cloud Computing: Advances, Systems and Applications, [online] Volume 8,11, pages 6-9. Available at: https://link.springer.com/article/10.1186/s13677-019-0133-z [Accessed December 2020].

AWS (2019). How can I check the integrity of an object uploaded to Amazon S3?. [online] Available at: https://aws.amazon.com/premiumsupport/knowledge-center/data-integrity-s3/ [Accessed December 2020].

Beet, N (2016). Cellebrite's UFED Cloud Analyzer Product Review. [online] Forensics Focus. Available at: https://www.forensicfocus.com/reviews/cellebrites-ufed-cloud-analyzer-product-review/?gclid=EAIaIQobChMIgdee-eT47QIVEJntCh06Gwa9EAAYASAAEgLLoPD_BwE [Accessed December 2020].

Diaby, T and Bashari Rad, B (2017). Cloud Computing: A review of the Concepts and Deployment Models. International Journal of Information Technology and Computer Science, Volume 6, Pages (51-55) Available at: https://www.researchgate.net/publication/317413701_Cloud_Computing_A_review_of_the_Concepts_and_Deployment_Models [Accessed December 2020].

Digital Forensics vs. OpenStack. (2016). [video] YouTube: Open Infrastructure Foundation. Available at: https://www.youtube.com/watch?v=cqZV3k0pUiw&feature=emb_logo [Accessed December].

Dykstra, J and Sherman, A (2013). Design and implementation of FROST: Digital forensic toolsfor the OpenStack cloud computing platform. Digital Investigation, [online] Volume 10, pages. Available at: https://reader.elsevier.com/reader/sd/pii/S174228761300056X?token=F0FD36FA153570EB78D80AE64C716CD6A0887E988659DF04349FC6F3AB55C6FCBF01B6C8130D310CBF58448640AF869E [Accessed December 2020].

ElcomSoft Co.Ltd. (2019). Elcomsoft Cloud eXplorer Manual. [eBook] Available at: https://www.elcomsoft.co.uk/help/en/ecx/hmcontent.htm [Accessed January 2021].

European Parliament (2006). Directive 2006/24/ec of the European Parliament and of the Council. Official Journal of the European Union, [online], pages 56-58. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [December 2020].

F-Response. (2017). F-Response Universal Manual 8.0.1.69 [PDF] pages 58-60. Available at: https://www.f-response.com/assets/pdfs/F-ResponseUniversalManualv8.pdf [Accessed January 2021].

Gartner (2019). Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019. [online] Available at: https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g [Accessed December 2020].

Grispos, G Storer, T and Glisson, W.B (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. International Journal of Digital Crime and Forensics, Volume 4, Issue 2, Pages 30-41 Available at:

https://www.researchgate.net/publication/235979829_Calm_Before_the_Storm_The_Challenges_of_Cloud_Computing_in_Digital_Forensics [Accessed December 2020].

Kene, S.G and Theng, D.P (2015). A review on intrusion detection techniques for cloud computing and security challenges. IEEE Sponsored International Conference on Electronics and Communication Systems, [online], pages 227-231. Available at: https://ieeexplore.ieee.org/document/7124898 [Accessed December 2020].

Naaz, S and Siddiqui, F. (2016). Comparative Study of Cloud Forensics Tools. Foundation of Computer Science FCS [online] Volume 5, pages 24-27. Available at: https://caeaccess.org/archives/volume5/number3/naaz-2016-cae-652258.pdf [Accessed December 2020].

National Institute of Standards and Technology (2011). The NIST Definition of Cloud Computing. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, Pages (2-3). Available at: https://csrc.nist.gov/publications/detail/sp/800-145/final [Accessed December 2020].

O'Shaughnessy, S and Keane, A. (2013). Impact of Cloud Computing on Digital Forensic Investigations. IFIP International Conference on Digital Forensics, [online] pages 1-17. Available at: https://www.researchgate.net/publication/283138811_Impact_of_Cloud_Computing_on_Digital_Forensic_Investigations [Accessed December 2020].

Pichan, A et al. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation, [online] Volume 13, pages 42-54. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1742287615000407?via%3Dihub [Accessed December 2020].

Quick, D and Choo KK. (2016). Big forensic data reduction: digital forensic images and electronic evidence. Cluster Comput, [online] Volume 9, pages 743-752. Available at: https://link.springer.com/article/10.1007/s10586-016-0553-1 [Accessed December 2020].

Roussev, V. (2009). Hashing and data Fingerprinting in digital Forensics. IEEE Security & Privacy, [online] Volume 7(Issue 2), pages 49-55. Available at: https://ieeexplore.ieee.org/abstract/document/4812157 [Accessed December 2020].

Ruan, K. et al. (2011). Cloud forensics: An overview. [PDF] University College Dublin, pages 2-14. Available at: https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview [Accessed December 2020].

Simou, S et al. (2016). A survey on cloud forensics challenges and solutions. Security and Communication Networks 9, [online] pages 1-25. Available at: https://www.researchgate.net/publication/310514661_A_survey_on_cloud_forensics_challenges_and_solutions [Accessed December 2020].

Simou, S et al. (2015). A Meta-model for Assisting a Cloud Forensics Process. 10th International Conference, CRiSIS, [online] pages 179-182. Available at: https://www.researchgate.net/publication/305475214_A_Meta-model_for_Assisting_a_Cloud_Forensics_Process [Accessed December 2020].

UK Legislation (2016). UK Investigatory Powers Act 2016. legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [Accessed December 2020]

UK Parliament (2020). Cloud Computing. The Parliamentary Office of Science and Technology, Westminster, London, Pages (1-3). Available at: https://post.parliament.uk/research-briefings/post-pn-0629/ [Accessed December 2020].

Vladimirskiy, V (2016). 10 Popular Software as a Service (SaaS) Examples. [online] Nerdio. Available at: https://getnerdio.com/academy/10-popular-software-service-examples/ [Accessed December 2020].

Watts, S and Raza, M (2020). SaaS vs PaaS vs IaaS: What's The Difference & How To Choose. [online] BMC Blogs. Available at: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/ [Accessed December 2020].

Zawoad S, Dutta A.K and Hasan R (2013). SecLaaS: Secure Logging-as-a-Service for Cloud Forensics. ASIA Conference on Computer and Communications Security, Hangzhou, China [online], pages 1-11. Available at: https://www.researchgate.net/publication/235712367_SecLaaS_Secure_Logging-as-a-Service_for_Cloud_Forensics [Accessed December 2020].

Zawoad, S et al. (2015). OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. IEEE 8th International Conference on Cloud Computing, [online] pages 437-441. Available at: https://ieeexplore.ieee.org/document/7214075 [Accessed December 2020].