The Impact of Cloud Forensic Readiness on Security

Ahmed Alenezi[1, 2], Nurul H. N. Zulkipli[1], Hany F. Atlam[1], Robert J. Walters[1] and Gary B. Wills[1]
[1]*Electronic and Computer Science Dept., University of Southampton, University Road, SO17 1BJ, Southampton, U.K.*
[2]*Computer Science Dept., Faculty of Computing and Information Technology, Northern Border University, Rafha, Saudi Arabia*

Keywords: Security, Digital Forensics, Cloud Computing, Cloud Security, Cloud Forensics, Cloud Forensic Readiness.

Abstract: The rapid increase in the use of cloud computing has led it to become a new arena for cybercrime. Since cloud environments are, to some extent, a new field for digital forensics, a number of technical, legal and organisational challenges have been raised. Although security and digital forensics share the same concerns, when an attack occurs, the fields of security and digital forensics are considered different disciplines. This paper argues that cloud security and digital forensics in cloud environments are converging fields. As a result, unifying security and forensics by being forensically ready and including digital forensics aspects in security mechanisms would enhance the security level in cloud computing, increase forensic capabilities and prepare organizations for any potential attack.

1 INTRODUCTION

It is agreed that cloud computing is increasingly acceptable and has brought many benefits to the field of computing. Cloud computing technology has allowed end-users to utilise technologies as services (Buyya, 2009). However, with the rapid adoption of cloud computing, it has become an attractive area for cybercrime, which leads to new technical and legal issues (Ruan et al., 2011). Since the introduction of cloud technology, extensive research has been conducted on cloud security, but cloud environments are still not compleately secure. The security concerns of cloud computing are: availability, privacy, integrity, and confidentiality. Once an attack occurs, digital forensics is concerned with finding, preserving, and analysing evidence, and providing reports, enabling the criminals to be prosecuted.

Since the quantity of cloud storage providers (CSPs) is expanding, users have numerous choices of services to store the data in the cloud (Yahya et al., 2014). However, the issue for keeping the safety of the sensitive data stored still important (Zissis and Lekkas, 2012). There are three recognised service models in cloud computing (Weinhardt et al. 2009; Ertaul et al., 2010; Mell and Grance, 2011) as shown Figure 1 (Zhang et al., 2010).

- Software-as-a-Service (SaaS) model – service providers offer their applications to users through the network. Users can access the applications using thin clients and browsers or program interfaces designed to communicate with the other applications hosted in the cloud.
- Platform-as-a-service (PaaS) model – mainly offered for applications developers as an environment on which to host and support development with libraries, services, tools, networks, and storage.
- Infrastructure-as-a-service (IaaS) model – provides the infrastructure and resources to host users' machines (virtual machines). IaaS providers offer computing power, storage, networks, and any other supporting resources to host virtual machines (VMs). Each host in the cloud IaaS model is occupied by a number of VMs sharing the resources; the VMs are isolated from each other by the virtualization layer.

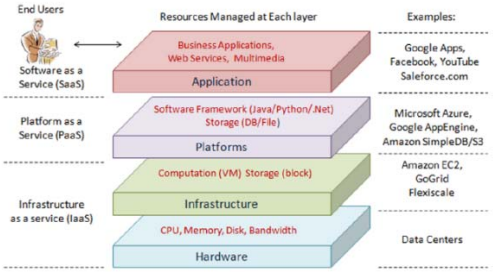

Figure 1: Cloud Computing Services (Zhang et al., 2010).

Alenezi, A., Zulkipli, N., Atlam, H., Walters, R. and Wills, G.
The Impact of Cloud Forensic Readiness on Security.
DOI: 10.5220/0006332705390545
In *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, pages 511-517
ISBN: 978-989-758-243-1

Four cloud deployment models described as Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud as shown in Figure 2. As discussed in (Fonseca and Boutaba, 2015) and (Jayaprakash, 2014), the deployment models can be described as the following:

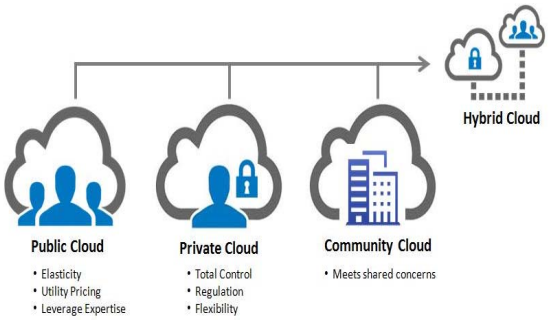

Figure 2: Cloud computing deployment models (Jayaprakash, 2014).

***Public Clouds*:** A cloud service provider offers their assets and resources including the administrations to the public. Public cloud offers a few key advantages to the service provider, including without bearing the cost of the infrastructure and the service provider will take full responsibility. However, this implementation of cloud needs subtle control over data and security settings, which impedes their capability in various organization (Fonseca and Boutaba, 2015).

***Private clouds*:** Also known as, internal clouds where it is Outline for the use by a particular organization. It permits the user to control the sort and design of equipment acquired. A private cloud might be constructed and overseen by the organization or by the external provider. The users have full control over execution, performance, dependability and security aspects of the cloud deployment. However, the flexibility scaling processing assets is reduced and no cost sharing choice due to single proprietorship (Fonseca and Boutaba, 2015).

***Hybrid Clouds*:** This type of deployment combines the public and private cloud models to complement each approach. It offers more flexibility. Hybrid cloud is firmly control and security over application data stood out from the public cloud, while yet reassuring on-demand advantage improvement and compression. A best practice is to utilize public cloud but leverages the private cloud where security and protection needs are too high (Jayaprakash, 2014).

***Community Clouds*:** A multi-tenant environment focused on a constrained set of organizations. These organizations meet up to share their computing resources and gain benefits. The organizations ordinarily have comparable security, protection, execution and consistency prerequisites. The people group, for the most part, confines members from a similar industry or with comparative needs (Jayaprakash, 2014).

2 CLOUD SECURITY

The cloud is increasingly acceptable but security concerns are being voiced about the implementation of this approach (Zissis and Lekkas, 2012). Users expect the cloud providers to provide suitable security controls (Subashini and Kavitha, 2011).

Cloud application software and databases are operated in large data centres. Sen, (2013) has summarized the following security issues:

- Threats in flaw of information resources
- Threat and attacker vector and their capabilities for attacking the cloud.
- Security risks related with the cloud (attacks and the countermeasures).
- Emergent of cloud security threats.
- Some cloud security incidents.

2.1 Current Attacks and Threats to the Cloud

Cloud computing is vulnerable to several types of security threat. Table 1 summarizes an outline of the threats and attackers to cloud service model and its

Table 1: Cloud Threats and Attacks.

Cloud Threats	Attacks on Cloud
Insider user threats	Malware Injection Attack: • SQL injection attack • Cross-sites scripting attack
External attacker & threats	Denial-of-Service attack
Data leakage	Side Channel attack
Data segregation	Authentication attack: • Brute Force Attacks • Dictionary Attack • Shoulder Surfing • Replay Attacks • Phishing Attacks • Key Loggers
User access Physical disruption Exploiting weak recovery procedures	Man-In-The-Middle Attacks: • DNS Spoofing • Session Hijacking

importance based on security requirement (confidentiality, integrity, and availability) as being discussed in (Sen, 2013), (Chou, 2013) and (Chouhan and Singh, 2016).

2.2 Cloud Security Risks

Few publications have addressed cloud security risks. According to Sen (2013) and Heiser and Nicolett (2008), Cloud security risks include:

- User access privileged
- Locality and division of the data
- Data removal
- Secure observation and e-investigations
- Assuring cloud security
- Compliance
- Availability
- Recovery
- Viability

3 CLOUD FORENSICS

Cloud forensics is an inter- discipline as it combines the cloud computing and digital forensic areas (Ruan et al., 2011). In cloud, there is a collective of networked data source that can be reconfigured rapidly with least effort (Mell and Grance, 2011). While in digital forensics, it is used to investigate and examine the potential evidence before presented in a court of law (Kent et al., 2006) when there is any potential of offense in a cyber-crime related to the cloud.

A more formal definition of digital forensic is presented by (Palmer, 2001) as follows:

" Digital forensics is the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Palmer, 2001).

The cloud forensic can be viewed as a subset of network forensic whew the investigation still being conducted using the main processes of network forensics but techniques deployed is personalized according to cloud computing environments (Ruan et al., 2011). Difference investigation procedures involve based on the service and deployment model of cloud (Zawoad and Hasan, 2013).

The Cloud Forensic Investigative Architecture (CFIA) is a model proposed by Ruan & Carthy (2013). It comprises the initial modules for allowing investigations in a cloud environment, as shown in Figure 3.

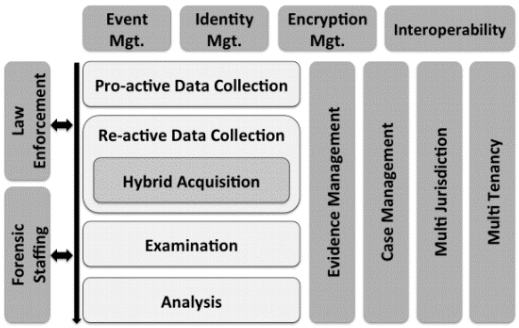

Figure 3: Cloud Forensic Investigative Architecture (Ruan and Carthy, 2013).

This model comprises four main divisions: 1) Pre-investigative Readiness, 2) Core-forensic Process, 3) Supportive Processes, and 4) Investigative Interfaces. In Figure 3, the vertical line is the component in cloud environment that being investigated, including the technical infrastructure and its legal complications. On the left side is the investigator team such as the forensic team or the law enforcement. At the top are shown the pre-investigation readiness components. The hybrid acquisition are the main forensic process modules where it collects a part of re-active data as includes in the of forensic acquisition techniques (Ruan and Carthy,2013).

3.1 Challenges in Cloud Forensics

The benefits and challenges in cloud forensic investigation has discussed in many previous works. Reilly et al., (2010) has concluded that having data in a central location is one of the benefits where the investigation can be carried out faster. (Grispos et al., 2012)

The challenges of cloud forensic usually related on how to control of the evidence, especially in the process of collection, preservation and validation. It is difficult to identify the evidence in the cloud environment since the deployment of service models is differ. Furthermore, seizing of the physical device that stores potential pieces of evidence is also restricted.

The challenges of cloud forensics is been listed by (Pichan et al., 2015) and (Grispos et al., 2012) according to the forensic phases in Table 2. From the list of challenges, the cloud forensic clearly require

new systems, structures and instruments for performing advanced investigation.

Table 2: Cloud Forensic Challenges (Pichan et al., 2015) and (Grispos et al., 2012).

Forensic Phase	List of Challenges
Identification	Obscure physical area Decentralized information Information Duplication Cross-Jurisdiction Reliance Chain Encryption Reliance on CSP
Preservation	Chain of Custody Evidence Isolation Dispersed Storage Information Volatility Information Integrity
Collection	Unavailability Reliance on CSP Trust Time synchronization Multi-Tenancy Cross-Jurisdiction Erased information Lack of investigation tools
Examination & Analysis	Absence of Log Framework Evidence time lining Encrypted information Coordination

The crucial challenge is that the evidence can exist in anywhere in the world. Any investigation needs to ensure that third parties have not compromised the evidence, in order to be admissible and acceptable in a court of law. (Grispos et al., 2012) In addition, it is also important to secure the chain of custody and maintain the integrity of the digital evidence.

Most of the cloud forensics techniques used depending on the cloud deployment and service model. For instance, the user does not have the ability to access the equipment in PaaS and SaaS, and they only rely on the logs provided by the CSP. While in IaaS, the end user have the capability to duplicate of the occurrence and obtain the logs (Zawoad and Hasan, 2013). The accessibility to the hardware and privacy differs between the public and private cloud where the end user is restricted to access those in public cloud and not in private cloud. (Subashini and Kavitha, 2011).

Cross-Jurisdictional aspects also become major challenges. In the modern distributed systems, the data might probable to go beyond national borders especially during the processing or storing of data sets. This challenge need to be considerable and it does not risk the investigative procedure (Pearson, 2013).

4 RELATIONSHIP BETWEEN SECURITY AND FORENSICS

There is no doubt that there is a relationship between security and forensics in the field of computing. Security concerns for cloud computing are: availability, privacy, integrity, and confidentiality, while digital forensics focus on finding and preserving evidence. It can be argued that digital forensics can facilitate and improve that security by its very readiness (Haggerty and Taylor, 2006).

Grobler and Louwrens (2007) acknowledged the existence of the overlap between security and forensics, and concluded that digital forensics components also can be considered as security best practices. Pangalos, Ilioudis and Pagkalos (2010) believe that the whole domain of security should be encompassed by digital forensics in order to have digital investigations that lead to successful litigation.

Marco, Kechadi and Ferrucci (2013) agreed that the readiness of digital forensics can enhance security since it prepares organisations to be ready for potential threats. Consequently, in cloud environments where digital forensics become more complicated, forensic readiness can be considered a noteworthy component of cloud security best practice.

4.1 Comparison of Cloud Security and Cloud Forensics

The key goal of security in cloud computing is to minimise the risk of potential threats and cyberattacks in the cloud, while digital forensics investigates any breach. The comparisons between cloud security and cloud forensics provided in Table 3.

Table 3: Comparison of cloud security with cloud forensics.

Cloud Security	Cloud Forensics
Aims:	
• Provides security assurance for both physical and logical security issues in cloud environments.	• Determines and reconstructs the chain of events that may led to a specific incident by analysing electronic information stored in the cloud.

Table 3: Comparison of cloud security with cloud forensics (Cont.).

Cloud Security	Cloud Forensics
Requirements:	
• Preparing the cloud infrastructure to support security. • Apply security controls, procedures, processes and standards. • Incident recognition e.g. Intrusion Detection Systems (IDS). • Security training and awareness. • Specify the judicial region and legal aspects in SLAs regarding security.	• Preparing the cloud infrastructure to support forensics. • Define forensics procedures, processes and standards. • Incident recognition e.g. Intrusion Detection Systems (IDS). • Forensics training and awareness. • Specify the judicial region and legal aspects in SLAs regarding forensics.
Pro-active:	
• Security measurements and preparations are considered in order to be securely ready to prevent cyber threats from ever happening in the cloud (e.g. meeting security requirements and applying set of procedures, processes and standards).	• Forensics measurements and preparations are considered in order to be forensically ready to undertake digital investigations in cloud environments (e.g. meeting forensics requirements and applying set of procedures, processes and standards.
Active:	
• Security responses and techniques to confront threats during a live incident.	• The ability to acquire digital evidence during real-time incident "live".
Re-active:	
• Security techniques to minimise and prevent further damage to the cloud (e.g. Disaster Recovery Plans).	• Investigative techniques after incident or while systems are inactive, to identify, extract, preserve, and analyse digital evidence.

4.2 Cloud Forensics as Part of Security

While many security experts believe that it is impossible to completely secure a system, Pangalos and Katos (2010) have emphasised the need to include digital forensics in security policies. This would obviously enhance the security since forensics typically rely on some security aspects, such as logs.

In cloud computing environments, a number of attempts have been made to include cloud forensics in security policies, but only in certain situations. However, in many cloud security breaches, a cybercrime has been committed, which should persuade both security and forensics teams to work together to minimise future threats and investigate the current cyber-attack. For example, security policies should state that when the IDS recognises a malicious activity, security and forensics teams need to be notified immediately. This would enhance the status of forensics readiness in organisations (Pangalos and Katos, 2010).

4.3 Cloud Forensics Readiness

Recent increases in the number of cyberattacks on cloud environments is clear evidence of criminals' ability to cause significant and costly damage to cloud customers or cloud providers (Marco et al., 2013). This increase in security breaches has encouraged many organisations to be forensically ready to undertake internal digital forensics investigations without relying on third parties (Hewling, 2013).

Being forensically ready would allow organisations to increase their ability to acquire admissible digital evidence and to reduce the costs of any potential digital forensics investigation (Tan, 2001). Cloud forensic readiness can be defined as preparedness to provide the relevant digital forensics information in order to increase the forensics capabilities and reduce the costs of carrying out cloud forensics investigations. In support of this, a cloud forensics survey has shown that three-quarters of the respondents agreed that collecting relevant data proactively in a cloud environment is important (Ruan et al., 2011).

There is a clear need for both cloud consumers and cloud providers to be forensically ready before any incident occurs, in order to minimise potential threats and investigation costs.

5 DISCUSSION

It is evident that there is a relationship between security and digital forensics in cloud environments. Despite the well-known fact that securing an entire system from potential cyber threats is almost impossible, many security and forensics teams in cloud environments are still working separately. Furthermore, a number of studies have confirmed that

digital forensics terms are missing from Service Level Agreements, standards and procedures (Ruan et al., 2012); (Thorpe et al., 2013); (Ruan et al., 2013); (NIST, 2014).

In many cases analysts' work relies on existing security techniques, which can lead to the acquisition of admissible evidence. This confirms the importance of teamwork among security and forensics, and the level of readiness and their contradictory objectives. For instance, by working together and intensively considering all the possible methods of digital attack, security practitioners can provide vital details to forensics analysts regarding what attackers may use and what preparations need to be made. Likewise, when an incident occurs, the security objective is to reduce the damages to the cloud in order to be available for other users, while the digital forensic objective is to acquire evidence and prosecute cybercriminals.

In order to close the gap between security and forensics in cloud environments, we recommend that organisations should be forensically ready. From the above discussion, it is evident that digital forensics readiness can certainly benefit cloud environments in many ways. Some of these benefits are cost effectiveness: where organisations do not need to hire external investigators (Ruan et al., 2011), being legal if law enforcement is engaged (Rowlingson, 2004), and improving security strategies (Pangalos el al., 2010); (Marco el al., 2013).

Once an organisation becomes forensically ready, digital forensics should be included in security policies. Unifying security and forensics together in cloud environments would increase the security level, and forensics capabilities, and make an organisation prepared for any potential attack.

6 CONCLUSIONS

While the volume of cyber threats is increasing, security in cloud computing is still an ongoing research area. Although cloud computing has become an attractive field for cybercriminals, no research has investigated the impact on security of cloud forensic readiness. This paper has introduced and compared the topics of cloud computing and digital forensics, in order to illustrate their overlap. Finally, the impact of cloud forensic readiness on the security level was discussed and how cloud forensic readiness can enhance cloud security. To reduce the gap between security and forensics in cloud environments, more studies need to be undertaken of readiness requirements and the factors that influence readiness. In the future, a case study will be conducted to demonstrate how cloud forensic readiness is used for particular cloud security incidents.

REFERENCES

Buyya, R. Yeoa, C. Venugopala, S. Broberga, J., Brandicc, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), pp.599–616.

Biggs, S. & Vidalis, S., 2009. International Conference for Internet Technology and Secured Transactions, pp.1–6.

Chou, T., 2013. Security Threats on Cloud Computing Vulnerabilities. *International Journal of Computer Science and Information Technology*, 5(3), pp.79–88.

Chouhan, P. & Singh, R., 2016. Security Attacks on Cloud Computing With Possible Solution. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(1), pp.92–96.

Ertaul, L., Singhal, S. & Saldamli, G., 2010. Security Challenges in Cloud Computing. S*ecurity & Management*, pp.36–42.

Fonseca, N.L.S. & Boutaba, R., 2015. Cloud Services, Networking, and Management. *In Cloud Services, Networking, and Management.* pp. 153–190.

Grobler, C. & Louwrens, C., 2007. Digital Forensic Readiness as a Component of Information Security Best Practice. *IFIP International Information Security Conference,* 232, pp.13–24.

Grispos, G., Storer, T. & Glisson, W., 2012. Calm before the storm: the challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics,* 4(2), pp.28–48.

Gary L Palmer. (2001). A Road Map for Digital Forensic Research. *Technical Report DTR-T0010- 01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).*

Heiser, J. & Nicolett, M., 2008. Assessing the Security Risks of Cloud Computing. *Gartner Research,* (June), pp.1–6.

Haggerty, J. & Taylor, M., 2006. Managing corporate computer forensics. *Computer Fraud and Security*, 2006(6), pp.14–16.

Hewling, M.O. (2013) Digital forensics: an integrated approach for the investigation of cyber/computer related crimes. *PhD thesis*. University of Bedfordshire.

Jayaprakash Ramsaran, (2014), Cloud Computing: Benefits and Challenges [ONLINE]. Available at: https://www.linkedin.com/pulse/20140921193928-23699310-cloud-computing-benefits-and-challenges [Accessed 15 December 2016].

Kent, K., Chevalier, S., Grance, T. and Dang, H., 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication*, (August), pp.800–886.

Marco, L. De, Kechadi, M.-T. & Ferrucci, F., 2013. Cloud Forensic Readiness: Foundations. *International*

Conference on Digital Forensics and Cyber Crime, pp.237–244.

Mell, P. & Grance, T., 2011. The NIST definition of cloud computing. *National Institute of Standards and Technology*, 53(6).

NIST Cloud Computing Forensic Science Working Group. (Draft NISTIR 8006), 2014. NIST Cloud Computing Forensic Science Challenges.

Pangalos, G., Ilioudis, C. & Pagkalos, I., 2010. The importance of Corporate Forensic Readiness in the information security framework. Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), *2010 19th IEEE International Workshop on. IEEE*, pp.12–16.

Pangalos, G. & Katos, V., 2010. Information Assurance and Forensic Readiness. *In International Conference on e-Democracy*. Berlin: Springer, pp. 181–188.

Pearson, S., 2013. Privacy, security and trust in cloud computing. *In Privacy and Security for Cloud Computing* (pp. 3-42). Springer London.

Pichan, A., Lazarescu, M. & Soh, S.T., 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, 13, pp.38–57.

Rowlingson, R., 2004. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, 2(3), pp.1–28.

Reilly, D., Wren, C. & Berry, T., 2010. Cloud computing: Forensic challenges for law enforcement. Internet Technology and Secured Transactions (ICITST), *2010 International Conference for*, pp.1–7.

Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M., 2011. Cloud forensics. *Advances in Digital Forensics VII, IFIP Advances in Information and Communication Technology*, 361, pp.35–46.

Ruan, K., Carthy, J. and Kechadi, T., 2011. Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis. *ADFSL Conference on Digital Forensics, Security and Law*, pp.55–70.

Ruan, K., James, J., Carthy, J. and Kechadi, T., 2012. Key Terms for Service Level Agreements to Support Cloud Forensics. *IFIP International Conference on Digital Forensics*, pp.201–212.

Ruan, K., Carthy, J., Kechadi, T. and Baggili, I., 2013. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, 10(1), pp.34–43.

Ruan, K. & Carthy, J., 2013. Cloud Forensic Maturity Model. *Digital Forensics and Cyber Crime*, pp.22–41.

Sen, J., 2013. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology*, (iv), p.42.

Subashini, S. & Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), pp.1–11.

Tan, J., 2001. Forensic Readiness. In Cambridge: *MA:@ Stake*, pp. 1–21.

Taylor, M., Haggerty, J., Gresty, D. and Hegarty, R., 2010. Digital evidence in cloud computing systems. *Computer Law & Security Review*, 26(3), pp.304–308.

Thorpe, S., Grandison, T., Campbell, A., Williams, J., Burrell, K. and Ray, I., 2013. Towards a forensic-based service oriented architecture framework for auditing of cloud logs. *2013 IEEE Ninth World Congress on Services*, pp.75–83.

Vaquero, L.M., Rodero-Merino, L., Caceres, J. and Lindner, M., 2009. A Break in the Clouds: Towards a Cloud Definition. *ACM SIGCOMM Computer Communication Review*, 39(1), pp.50–55.

Weinhardt, C., Anandasivam, D.I.W.A., Blau, B., Borissov, D.I.N., Meinl, D.M.T., Michalk, D.I.W.W. and Stößer, J., 2009. Cloud Computing - A Classification, Business Models, and Research Directions. *Business & Information Systems Engineering*, p.391.

Weiss, A., 2007. Computing in the Clouds. *netWorker Magazine - Cloud computing: PC functions move onto the web*, (Volume II, Issue 4), pp.16–25.

Wolthusen, S.D., 2009. Overcast: Forensic discovery in cloud environments. In IMF 2009 - *5th International Conference on IT Security Incident Management and IT Forensics* - Conference Proceedings. pp. 3–9.

Yahya, F. et al., 2014. Security Challenges in Cloud Storage. *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*.

Zawoad, S. & Hasan, R., 2013. Digital Forensics in the Cloud. *CrossTalk*, (October), pp.17–20.

Zawoad, S. and Hasan, R., 2013. Cloud forensics: a meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv*:1302.6312.

Zhang, Q., Cheng, L. & Boutaba, R., 2010. Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), pp.7–18.

Zissis, D. & Lekkas, D., 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), pp.583–592.