Importance of Reliable and Secure Cloud Networks

**41001 Assignment 1**

**Harrison Jeffs - 12966370**

**Yeaseul Jeong - 13659661**

**Michael Ryo Kandiawan - 13407123**

# Table of Contents

[Table of Contents 2](#_Toc39309901)

[1. Abstract 2](#_Toc39309902)

[2. Introduction 3](#_Toc39309903)

[2.1 Introduction to Reliable and Secure Cloud Networks 3](#_Toc39309904)

[2.2 Overview 3](#_Toc39309905)

[2.3 Keywords 4](#_Toc39309906)

[3. Summary 5](#_Toc39309907)

[4. Reflections 9](#_Toc39309908)

[5. Bibliography 11](#_Toc39309909)

# Abstract

This report will cover a standard explanation of security within cloud computing, more specifically the importance and regulation of reliable security within cloud computing.

Security is essential in protecting the privacy of important data stored and located within cloud networks, therefore making it one of the more important aspects of cloud management for developers.

We researched numerous informative and descriptive articles and webpages that delve into the fundamentals of security within Platform as a Service and have devised this report to properly elaborate on key information to support our knowledge. We plan to utilise these well-written resources to describe and formulate a report detailing the different aspects of reliable security systems and environments currently present in the cloud computing industry. We hope this report will provide a comprehensive and informative research port covering various forms of security implementation within cloud based platforms.

# Introduction

2.1 Introduction to Reliable and Secure Cloud Networks

Cloud computing networks and systems are becoming more essential in our modernized world as the reliance on internet-based data storage and content handling covers a majority of all web servers and sites accessible world-wide.

Therefore, ensuring that these highly complex networks of systems are constantly performing is essential. The reliability and security are the most important factors when regarding cloud systems. Without stable and reliable worldwide systems to analyse and maintain data, many websites and online services will fail, leaving customers and businesses alike without access to important data.

2.2 Overview

Cloud computing concerns the storage and management of data on a network of private or public remote servers, as opposed to on-site physical storage. This eliminates the process of requiring one’s own storage servers, but faces numerous risks as consumers must consider the validity of the cloud services they trust to keep their data secure. Cloud computing requires high levels of both reliability and security to function properly, to retrieve large data from network servers whilst maintaining its privacy and preventing data theft through intense security measures. Dealing with important personal and corporate data, cloud providers need to ensure that they are running at the highest quality in order to secure data and remain prominent amongst competitors. The security and privacy of data in cloud-based services is paramount to the performance of the system and reputability of the provider.

Security as a Service (SECaaS) is a term used to describe the providing of subscription based security infrastructure to corporate cloud networks. Security as a service is a method that provides high quality security measures to clients in exchange for subscription payments. The maintainability of the security structure is within the interest of both parties, though primarily the main responsibility of the provider.

Cloud computing has provided organisations to outsource in networking, servers, storage, virtualization, operating systems, runtime and data applications in technology stack (SumoLogic, 2020). Cloud computing has also brought increased greater reliability, immense scalability and also it declined costs and changed the outlook of computing.

However, there are numerous challenges to face within cloud computing environments. In contrast to the benefits that the cloud computing could offer, Tripathi & Mishra (2011) suggest that it is important to develop appropriate security for implementations against cyber-attacks, data theft and other threats. Organisations should consider privacy, security, reliability, accessibility and regulation issues and be aware of the risk of data breaches in cloud environments. Securing computing infrastructure and stable security is not achieved in one-shot but it requires more ongoing effort. Due to these reasons, it is critically mandatory to analyse and update up to the state-of-the-art security (Ahmed & Hossain, 2014).

Both security and reliability play their respective parts in the development and maintenance of a high quality industry-grade cloud network, be it Platform or Software as a Service (PaaS, SaaS respectively). Without vital attention to these criteria, networks will face countless data issues.

2.3 Keywords

**Data -** Important digital information belonging to personal users, clients and businesses

**Security -** The ability of the network to maintain the privacy of one’s data - to keep data safe and accessible only to those granted access

**Reliability -** The quality of performing to a highly considerable standard consistently

**Trust -** The user and client’s ability to believe that their data is secure in the cloud network they choose

**Cloud -** A virtual network of remote servers to host, store and manage data

# Summary

When dealing with the increased load of private information cloud-based networks must deal with on a regular basis, implementing strong security infrastructure is absolutely essential. Reliability is consistently recognized as highly essential in any system and providing these services helps client confidence and satisfaction (Mesbahi et al). Based on the research of Mesbahi et al, “The probability that a system is operational in a time interval without any failures is represented as the system reliability”.

The reliability of a system is directly related to how well it operates over a lengthy period of time. Given the necessity of data recollection when accessing cloud-based networks, it is safe to assume that a system that can be deemed ‘reliable’ is one that is consistently accessible at any given time. Network down-time is a factor that can damage the reliability considered of a system.

Meshbahi states that “Cloud computing service outage can seriously impact workloads of enterprise systems and consumer data and applications” (Mesbahi et al), and this is proven through numerous examples, including the April 2011 Amazon EC2 outage. Referred to as one of the largest cloud outages, this outage caused widespread disruption to websites, such as Reddit and Quora, running off the AWS EC2 infrastructure. This led to major data loss, which was a devastation for such large websites. The importance of stable and functional network systems and architecture is proven, as even short outages can have detrimental effects on personal data. System reliability needs to be taken into account before release to the public. Meshbahi’s article gives thorough details and covers different aspects of how reliable services are considered to be essential in regards to cloud systems.

[Izrailevsky](https://www.computer.org/csdl/search/default?type=author&givenName=Yury&surname=Izrailevsky)’s (2018) paper ‘Cloud Reliability’ ([Izrailevsky](https://www.computer.org/csdl/search/default?type=author&givenName=Yury&surname=Izrailevsky) et al) also uses examples of reliability issues to its advantage, detailing the 2012 Netflix outage which left customers without service for 18 hours, leading them to consider a change to Active-Active cross regional architecture, to ensure the issue would not prevail. These choices of platforms in regards to functionality and performance are necessary to maintain client and customer satisfaction (Izrailevsky, 2018).

[Iankoulova](https://www.researchgate.net/scientific-contributions/2007704402_Iliana_Iankoulova)’s article ‘Cloud Computing Security Requirements’ covers the importance of security integration in a cloud network. In regards to previous articles, it touches on how essential reliable security software and services are for the insurance of the security of data. Despite being an 8 year old article, the paper covers common aspects of cloud that still holds to this day.

As the cloud computing networks become more virtualized, organisations are losing control of physical access to the cloud server which has the host’s sensitive data. This makes the organization more vulnerable in determining who has physical actual access to the servers (Jathanna & Jagli, 2017). Lack of visibility of applications and services which has low transparency could hinder organisations to collect or aggregate data efficiently about the security status.

Similarly, prominent flexibility of data location in the cloud raises security concerns. Thus gaining transparency of data location and knowing the specific location of data storage are crucial for securing user’s personal data in cloud computing environments to be able to provide appropriate data protection (Ahmed & Hossain, 2014). Other than technical aspects, the authors (2014) point out that trust is another important factor that could reduce security concerns. It is because trust in the cloud environment is a most influential soft factor due to the responsibility in auto managing, processing and building credibility and authenticity. Credibility and authenticity of the cloud service providers are key elements establishing a successful cloud computing environment.

Jathanna & Jagli (2017) emphasized that while cloud services interact with API to manage and monitor the cloud provisioning there are also occurrence of the security issues. When the third parties rely on APIs to build interfaces, the risk increases when they need to reveal more services and credentials. Security relevant issues such as confidentiality, accountability and availability could be deteriorated due to the interaction between APIs and weak interfaces which allows external parties to access from open internet.

Keeping data secure and confidential is the most vital aim for the customers when moving to cloud. Thus, it is crucial for the users and provider to know specifically who creates data, where data is stored, who can access and change data, phase after the data is deleted, how the backup works and how to transfer data (Omega-Neamtiu, 2012).

SumoLogic (2020) determined 4 categories of cloud computing security controls. Deterrent controls are constructed to discourage vicious actors from degrading cloud systems and also work as a warning for an attack that will cause severe consequences. Such as cloud service providers could be a deterrent subject when checking on criminal background on employees. By eliminating vulnerabilities, preventative controls make the cloud environment more flexible by writing codes to disable inactive ports to exclude other available entry points for attackers. Detective control detects and reacts to the treats and intrusions by monitoring the network security with detection software. Lastly, corrective controls could limit damage in the event of a security attack. Data servers are detached from the network when a developer writes code after detecting a threat to prevent a data breach.

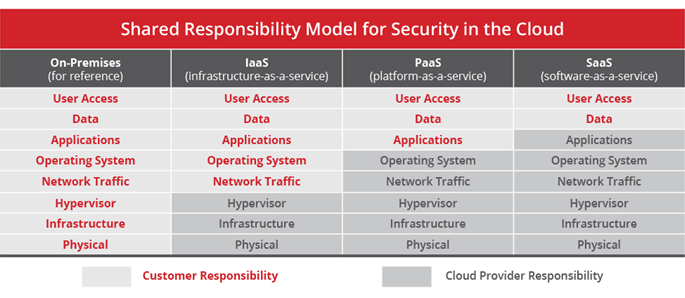
Other than security controls, there are two more ways to obtain a safe cloud environment. It is important to keep in mind that to protect account credentials from being stolen, organisations should not share account credentials among users and services so that all the transactions can be traced and monitored. Furthermore, to solve external malicious threats, data encryption can help. Because unencrypted data is vulnerable and not suitable for security mechanisms. Unauthorized users could access through unencrypted data and it is putting servers at risk by leaking data and encouraging the malicious users to misuse the data. In the case of a real world example, Dropbox was accused of using one encryption key for all users’ data stored in the Dropbox servers (Jathanna & Jagli, 2017).

Policies and procedures exist within cloud security to protect all cloud systems and infrastructure from both attacks and breaches. To support customer’s data and privacy, customers need good security. By using authentication and traffic filters it can increase cloud security. However, cloud security is a shared responsibility by the user and provider. Security is important because all the data and important files need to be secured so only the administrator can access it. (Forcepoint, n.d)

In regards to security, users and providers share the responsibility to protect any data. Both parties need to work to reduce and potentially eliminate various types of risk by enabling, data recovery, encryption, etc. Some of them also secure their data by using a warning to the attacker to remind them of the consequences. This also works to discourage the attacker before they start attacking. They could prevent the attack which will reduce the chance to get an attack. Using a good authentication system will reduce a chance for a public user to access the data. They also identify the attack by monitoring network traffic. This technique could help them to predict when an attack comes. The last technique is to limit the damage from an attack. By creating a code that will automatically disconnect the data server when the attack comes will prevent data theft from happening. (SumoLogic, n.d)

Cloud computing use and implementation is currently growing in Information Technology based organizations. It creates a new challenge in terms of securing data which could not be identified or solved using traditional network technique. It is also difficult to trust a cloud provider since the employee itself could illegally modify or copy the data to others. Therefore, it is better if they could apply transparent control to the server. (SumoLogic, n.d)

As we have said before accessibility is a quite big risk because cloud providers secure data by using username and password but there is a risk for the attacker to gain password and username. Therefore, the provider itself should increase security by using an access management system. The other reason usually people got attacked is because they have a lack of control over the cloud itself. This makes customers need to rely on the cloud provider as an administrator for some of the decisions. (McAfee, n.d)



*Figure 3.1 – Shared Security Responsibility between User and Provider (McAfee, n.d)*

There are several problems that commonly happen in SaaS. It is also possible for the theft attack to the SaaS provider by attacking them. Therefore, we should also set better security on the SaaS provider or choose a good provider that gives better security. These are some of the security problems that usually happened to either client or provider. (McAfee, n.d)

* Lack of visibility into the data inside the cloud application.
* Incomplete control for the user to access important data.
* Data theft.
* Not able to monitor the data transmission inside the cloud.
* Lack of security expert
* Lack of power to prevent insider theft the data

On the other hand, IaaS usually gives the customer less restriction than SaaS. In this case, it also gives the customer a bigger responsibility through their data. So, it is very important to control accessibility to prevent data theft. To prevent the security problem happening, it is important to check abnormal behaviors that come through a network, also securing the network traffic. There are several security problems that have been experienced by a user or provider. (McAfee, n.d)

* Lack of security controls.
* Advanced attack to the cloud provider
* Low skill on monitoring network
* Spread attack on the cloud.
* Lack of security expert

# Reflections

Based on our research, it would seem rather obvious at first glance that an efficient security model and reliable performance records would be the quint-essential aspects stakeholders would consider when it comes to operating and maintaining cloud systems. The importance of data privacy and availability are the key components to a strong business model when referring to these networks.

In regards to Platform as a Service, downtime can have drastic effects on the performance and stability of the systems and services running off the network, which is why clients are encouraged to choose stable and reliable services, and why reliability is so important in this regard.

Based on the research, common crisis cloud computers are facing are that cloud services are now opening new dimensions to threat apart from phishing, fraud and software exploits. In a cloud environment, attackers can easily eavesdrop on activities, manipulate transactions, modify data and use cloud applications to launch unprecedented malicious attacks (Jathanna & Jagli, 2017).

Apart from the technical aspect, it was interesting to realise malicious activities from inside intruders can possibly harm confidentiality, integrity and availability of most of the data and services, internal activities and organisation’s reputation along with customer’s trust (Omega-Neamtiu, 2012). As well as external hackers, unauthorised internal employees easily accessing data either intentionally or accidentally can be a possible threat that is against the implementation of better security mechanisms in cloud computing environments. 21 % of cyber-attacks were caused by insiders according to the 2011 Cyber Security Watch Survey. Mostly, unauthorized users intrude on the victim's IP address to use corporate information and steal intellectual property which lead to data breaches. In cloud one unauthorized user could destroy entire infrastructures (Jathanna & Jagli, 2017).

It was surprising to find out that fundamental elements of cloud computing can put cloud computing security at risk. IaaS which provides fundamental functionality of an entire cloud ironically gives an ideal platform for hackers to perform attacks (Jathanna & Jagli, 2017). Virtual machines that are working on top of IaaS can be also misused for causing data breach. With the advent of multi-tenancy, it turned out that people are generating new attack surfaces by sharing memories, databases and resources with each other. The authors (2017) could tell the susceptibility in systems and exploitable bugs in programs become more fatal problems in cloud computing.

Throughout the research some intriguing facts were that not only the users or customers but also developers may face the complexity of building secure applications in the cloud. So, it seemed crucial for the developers to be educated and informed about data legal issues in order not to store data in inappropriate locations. When data is stored in different places with different legal regimes that incur its privacy and security issues (Jathanna & Jagli, 2017).

After the research, sufficient data backup and prompt disaster recovery are very important when it comes to face data loss. In the past, cloud data centers were vulnerable to attacks which deleted all data permanently in the cloud to cause business harms. Cloud service providers should distribute applications and data across the multiple zones and have daily data backup and off-site storage. Furthermore, for the data provider, before uploading it on the cloud, customers should always encrypt data and also to carefully protect encryption keys in order to keep sensitive data safe (Jathanna & Jagli, 2017). However, Jathanna and Jagli (2017) warn that when cloud networks are regularly backed up without encryption, this could lead to misuse of data and various security threats so it still needs to be treated with caution.

Even though there are solutions for cloud computing, cloud environments are still vulnerable to security issues like cloud malware injection attack, browser security issues, flooding attacks, locks-in, incomplete data deletion, and data protection.

# Bibliography

Ahmed M, Hossain M 2014, *Cloud Computing and Security Issues in the Cloud,* viewed 18th April 2020

<https://www.researchgate.net/publication/276199301_Cloud_Computing_and_Security_Issues_in_the_Cloud>

Florin Ogigau-Neamtiu 2012, *Cloud Computing Security Issues*, viewed 21st April 2020

<https://core.ac.uk/download/pdf/27177466.pdf>

Forcepoint n.d, *What is Cloud Security?,* viewed 17th April 2020

<https://www.forcepoint.com/cyber-edu/cloud-security>

[Iankoulova](https://www.researchgate.net/scientific-contributions/2007704402_Iliana_Iankoulova) I, Daneva M 2012, *Cloud Computing Security Requirements: A Systematic Review,* viewed 16th April 2020

ht[tps://www.researchgate.net/publication/261038126\_Cloud\_computing\_security\_requirements\_A\_systematic\_review](https://www.researchgate.net/publication/261038126_Cloud_computing_security_requirements_A_systematic_review)

[Izrailevsky](https://www.computer.org/csdl/search/default?type=author&givenName=Yury&surname=Izrailevsky) Y, Bell C 2018, *Cloud Reliability,* viewed 13th April 2020

<https://www.computer.org/csdl/magazine/cd/2018/03/mcd2018030039/13rRUxcsYO5>

Jathanna R, Jagli D 2017, *Cloud Computing and Security Issues,* viewed 10th April 2020

<https://www.researchgate.net/publication/317908867_Cloud_Computing_and_Security_Issues>

McAfee n.d, *Cloud Computing Security Issues and Solutions,* viewed 15th April 2020

<https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html>

Mesbahi M, Rahmani A, Hosseinzadeh M 2018, *Reliability and high availability in cloud computing environments,* viewed 9th April 2020

<https://hcis-journal.springeropen.com/articles/10.1186/s13673-018-0143-8>

SumoLogic n.d, *What is Cloud Computing Security? Cloud Computing Security Explained,* viewed 21st April 2020

<https://www.sumologic.com/glossary/cloud-computing-security/>

Tripathi A, Mishra A 2011, *Cloud Computing Security Considerations*, viewed 22nd April 2020

<https://ieeexplore.ieee.org/abstract/document/6061557/>