[Introduction 1](#_Toc1815247527)

[Chosen Research Topic 2](#_Toc298960974)

[Chosen Research Principle 2](#_Toc929721015)

[Methods for Research Techniques 3](#_Toc1562054062)

[Web Articles in Cloud Computing Security 4](#_Toc1586319298)

[Literature Review – How have recent security breaches showed a lack of Cloud Security improvement? 4](#_Toc1812729027)

[Conclusion 6](#_Toc723549275)

# Introduction

The first section of the report covers a chosen Cyber Security industry which will be Cloud Computing Security and then answers a critical question. Cloud Security was the chosen topic because it has a lot of time left before it is perfected. Being able to use computers in the cloud is also a newer technology. The report will then follow on by giving an insight as to what research principles are and which ones will be used for the final part. The chosen principles will be Primary and Secondary techniques. These were chosen because their methods of gathering information link well with the computing industry. After going into further detail about primary and secondary research methods, the skills will be applied to the question *“How have recent security breaches showed a lack of Cloud Security improvement?”* Although the massive PlayStation was a while ago, it gives a good comparison to the more recent attack of Toyota in June 2023. It gives a good scope on what methods were available to prevent and how Toyota messed up.

# Chosen Research Topic

For this assignment, the topic that will be covered is cloud computing security (CCS). According to Amazon Web Services *(AWS, 2023),* cloud computing allows users to access computer devices (like servers, storage, software, etc.) over the internet. Instead of buying and owning physical hardware and software, people can use these services whenever they need them from companies that provide cloud technology. Examples of these companies are Nvidia and Google. The reason cloud computing was chosen is because it’s upcoming and its capabilities haven’t been fully discovered yet therefore it’s imperative that its security is up to standard.

*(IBM, 2023)* says that it also offers major benefits such as data management, optimisation of resources as well as being an environmentally friendly platform. It lets researchers concentrate on their research outcomes without the limitations of hardware.

# Chosen Research Principle

The main principle that will be used is Primary/Secondary techniques. Smart Survey *(smartsurvey, 2023)* describes Primary principles as research techniques that directly gain information. Examples include questionnaires, Observations, and experiments. According to *(Qualtrics, 2022),* the Secondary techniques help the researcher gain information based on the data gathered from the primary techniques. Some types of secondary principles can be benchmarks and market/data analysis.

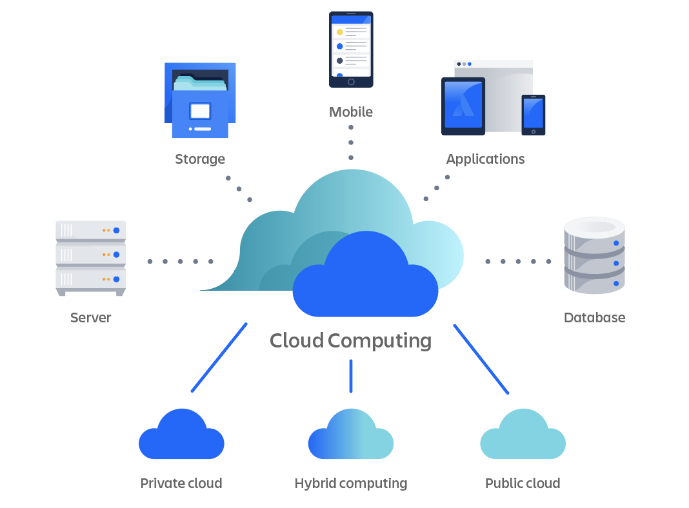
These research principles can help the development of cloud security from a business standpoint. Companies can use these techniques to create a better user experience for consumers.

For the Primary techniques like questionnaires, they can help companies improve their cloud computing services. They could ask questions like:

How secure do you feel when using our cloud computing service?

How satisfied are you with the overall performance of our systems?

Do you feel our services are too expensive for your current use time?

Based on these answers they may use secondary techniques like market analysis to conduct even more research. They could then:

Improve security of cloud systems

Consider server location changes.

lower cost which may influence companies.

# Methods for Research Techniques

There are many methods of Primary research techniques that can be used to improve the security of cloud computing. Some include:

Questionnaire – A set of questions that aim to gain information about research topics.

Surveys – a broader method of research that includes questions alongside other processes to gain information about a bigger audience.

Case Study – This analyses a specific demographic and how their behaviors link with the research topic.

From what SurveysDriect has found surveys have played a huge role in rapid development of cloud computing’s security. *(Surveysdirect, 2016)* As mentioned before, cloud computing comes in many different forms and conducting surveys will help focus security on the areas that need it the most.

For example, Apple wanted to know how to implement their new cloud security technology. They asked questions based on whether they use cloud computing for storage, gaming, or anything else. They concluded that storage is the least secure aspect and add 2 factor authentication to their cloud storage login page. This massively helps cloud security because it puts trust in the community which will attract more users.

A screen shot of a login

Description automatically generated

Secondary research techniques are usually based off the information gathered from the primary methods. Examples include:

Research reports – a report that details and summarises the findings of research on a topic.

Meta – analysis – like a research report, however it takes the results from multiple primary research techniques and compares them to achieve a varied answer.

Article (web/newspaper) – content that is either uploaded to the internet or added to a newspaper that gives facts, statistics, or opinions on any topic.

## Web Articles in Cloud Computing Security

A web article would be a great follow up tool to implement after conducting research via a primary technique like a survey. As mentioned before, a company like Cisco could create a survey to better the security for cloud technology. For this information to reach more people, and more companies, they could publish a web article based on their results. Since there is a large amount of people who read on the internet, it could lead to competitors seeing it and making upgrades to the security of their cloud computing technologies. Thus, creating a more secure cloud for customers to access.

A Secondary benefit of web articles in CCS is increased Threat Intelligence. Informing people of the specific vulnerabilities that the experts researched will also help bring awareness to the casual users. This could massively aid in the prevention of cyber-attacks on the cloud. E.G: Lookout.com have created a web article called “the top 5 risks when operating on the cloud” *(lookout, 2023).* It highlights key issues which people should be aware of, everyone reading the article would be informed to implement safety measures which would also increase the security of using computing technology on the cloud.

A screenshot of a computer

Description automatically generated

# Literature Review – How have recent security breaches showed a lack of Cloud Security improvement?

The infamous PlayStation Network Hack (2011) and the Toyota Data leak (2023) are two good comparisons to show how there needs to be a bigger push for cloud security to keep user’s data out of harm’s way. Arcserve says that 39 % of businesses experienced a data breach last year and 40% of the cloud data was sensitive. *(Arcserve, 2023)*.

A newspaper with a person walking in front of a door

Description automatically generatedWhat exactly happened in the PSN hack? Around 77 million PlayStation users logged in to notice their accounts were compromised. As well as accounts, banking information may have also been included in the data. *(WSSwired, 2021).* They then had to announce that they had a net loss of around $140 Million which was the greatest loss for a company due to a cyber-attack at the time thus resulting in major investors not wanting to do business with them since their IT security was so low. Worldwide news of the attack spread, causing various newspapers to publish articles on the event, further damaging their reputation.

Figure 1, Newspaper Article alerting the public about the hack

In terms of the Toyota Hack, the whole issue stemmed from an incorrectly configured cloud storage location, allowing hackers to steal the vehicle information of around 200,000 users. Data such as “In-vehicle device ID, map data updates, updated data creation dates, and map information” were externally accessed *(CSOonline, 2023)*. This is already a bad sign which indicates to a lack of improvement in Cloud Security over the years. For a company on the scale of Toyota, these mistakes can be extremely costly, and they were. Despite not releasing the figures of the financial damage they ensured, it’s safe to say they would have received: reputational damage causing them to lose customers, extra costs to increase their security and fines due to the violation of certain data laws.

This proves that Cloud Security hasn’t improved since the PSN data breach because the fashion in which both companies were attacked in is too similar. When the PSN hack occurred, data security techniques were not as developed and widespread. Toyota showed a distinct lack of knowledge in configuring secure storage location. *(SecureFrame, 2023)* released statistics that showed “even though 92% of people are aware of same password risks, 65% always or mostly use the same password”. A company as big as Toyota should be leading by example as a business who knows and understands the importance of cloud security when it comes to customer data. To give credit to Toyota, they were not isolated in their cloud attack. Expert Insights published an article which mentions that out of every data breach in the past year “45% of them are cloud-based”. They also find out that 80% of companies have experienced “at least one cloud security in the last year” *(expertinsights, 2023)*. This doesn’t help with the overall point of the literature review. Too many companies have failed to spot the tell-tale signs that PlayStation were not able to discover in time.

So how should companies effectively set up their cloud services to avoid data breaches? A magazine from SECURITY was published that says the main thing a business must do is “partner with a trusted provider” *(SecurityMagazine, 2020)*. The idea of linking with a business whose sole purpose is to provide a more secured version of a platform can be beneficial and would help in a push for improved cloud security. According to a survey from Cloudwards, the most secure options are Sync.com, pCloud and IceDrive. *(Cloudwards, 2023)*.

To put it shortly, yes. The Toyota breach highlighted how there’s standstill in security in terms of Cloud Security and their needs to be a bigger push for the protection of user data. Bigger companies also need to be held accountable for poor Cloud Security choices. ‘StickmanCyber’ explains private clouds have “sole responsibility of security vested in the corporation” *(stickmancyber, 2022)* Furthermore, the PSN data breach needs to be analysed further so that other companies can take note of the mistakes made and put effective precautions in place.

In summary, the major PSN breach has not been analysed enough in the cloud security industry and its long-term implications are still affecting companies in the present day 2023. If there was a bigger push for cloud security and a better understanding of what caused the breach 10 years ago, Toyota would not have suffered such a loss. Both companies would have also suffered financial, reputational, and operational losses. This is because they would have had to expend extra resources to deal with the attack. These 2 companies should also be at the forefront for the cloud security push as this can encourage other business to follow secure techniques such as Trusted Provider partnerships.

# Conclusion

To round up everything this assignment has covered: Cloud Computing gives users the power to access computer technology completely virtually and without owning any of the hardware. This means they also need to be secured like a normal desktop with various methods. To find out how secure cloud computing is, research must be conducted. One way of doing this is through primary and secondary research techniques. Primary methods give someone direct information about something such as a questionnaire. Secondary methods give information based on what was gathered from the primary research. One example can be a journal. These techniques can be used to prove how there has not been a big enough push for Cloud Security since one of the biggest data breaches, the PlayStation Network breach. This lack of a push also resulted in Toyota suffering a massive breach in the present day 2023.

Sources:

PSN Hack newspaper article

Toyota Data Leak Report based on the damages

Example of proper cloud security practices

Analytic report of data lost during Toyota 2023 hack

Toyota site – official apology notice

How to safely store accounts in the cloud – beyondtrust.com