Bachelor Degree Project

Assessing Practices of Cloud Storage Security Among Users

A Study on Security Threats in Storage as a Service Environment

Authors: Hugo Joo Jonsson, Vilgot Karlsson
Supervisor: Arianit Kurti
Examiner: Ola Flygt
Semester: VT 2023
Subject: Computer Science

Abstract

With the immense amount of data generated daily, relying solely on physical storage is insufficient. Therefore, Cloud services have become a big part of our day-to-day life, as they allow users to store data and relieve customers from the burden of maintenance. However, this technology relies on the internet, which increases the potential security risks and threats. This survey-based study investigates users' security practices concerning Storage as a Service, along with a literature review of current security threats targeting users of these services. Additionally, a comparative analysis is conducted to compare the security features offered by the cloud storage providers. The study shows that users are generally concerned about internet security, and service providers have implemented appropriate security features to protect users.

Keywords: Cloud Computing, Storage-as-a-Service, Security threats, Security practices

Preface

First and foremost we would like to thank our supervisor, Arianit Kurti, that has supported us throughout this bachelor thesis work. Without his continuous support, we would not have been able to complete our work within the time period. We would also like to thank Ola Flygt for being our program coordinator, who has inspired us throughout this bachelor's degree program in network security. Lastly, we would like to thank all the respondents that have taken the time to answer our survey and made this thesis possible in the first place.

Contents

1 Introduction

This 15 HEC bachelor's degree thesis in computer science, and has been done in pairs and will be exploring users' cloud storage security practices. Hugo Joo Jonsson has written the chapters and potential sub chapters Introduction (1), Theoretical Background (3), Threats Against Cloud Storage Users (3.3), Research Implementation Comparative Analysis (4.2), Result (5), Result Cloud Storage security practices Survey (5.1), and Analysis Cloud Storage Security Practices Survey (6.1). Vilgot Karlsson has written the chapters and potential sub-chapters Method (2), Theoretical Background Cloud Computing (3.1), Theoretical Background Security Policies (3.2), Research Implementation Survey Overview (4.1), Result Comparative Analysis (5.2), and Analysis Comparative analysis of Storage as a service (6.2). Subsequently, the literature review, survey, and comparative analysis have been conducted and executed together, but where Hugo had a deeper investment in the survey while Vilgot focused on the comparative analysis. The literature review was done together and the work was split 50-50.

Internet users all over the world generate a large amount of data, and that data needs to be stored or saved somewhere. The old ways may not be sufficient anymore, and cloud-based storage may be the solution. All data that is created regardless of type, needs a storage device and a storage method to store and maintain the data. There are two main categories of storage devices, Direct Attached Storage (DAS), and Network-Based Storage [1]. The Direct Attached Storage, as the name suggests is a storage device that is directly connected to the device that is using it. The machine or device that is using or accessing the storage medium frequently shares space with the storage device and is directly connected to it. The direct-attached storage can provide a decent lookup speed but has limitations when sharing the stored information since Direct Attached Storage devices only allow for one machine to be connected/attached to the storage device at a time [1]. Direct Attached Storage devices come in many different forms, and the two most commonly used ones are Hard Disc Drives (HDDs) and Solid-State Drives (SSDs). Several Direct Attached Storage devices have been faced out due to their inferiority to the HDDs and SSDs when it comes to storage capacity and read/write speed [2]. A better option for data sharing and collaboration between machines on a network is network-based storage, a type of data storage that enables access to the stored data by machines or devices over a network. The off-site storage nature of the solution makes it better suited for backup and data protection rather than traditional data storage. There are different kinds of Network-Based Storage and two commonly used ones are network-attached storage (NAS) and storage area network (SAN) [1, 3].

Alongside the upspring of cloud computing comes the Storage-as-a-service (StaaS) model or also known as cloud-based storage alongside many other service models. The cloud-based storage allows users to store their data at a third-party cloud computing provider that they can access through a public or private network connection [4]. Cloud

storage providers use remote servers containing several virtual machines to store and maintain user data. The storage solution give the user great availability of their stored data and at the same time provides easy and fast scalability of the storage capacity the user has from the provider [5].

Cloud-based storage has become popular since the user pays a fee to get access to a provider's service and the user does not need to set up or manage anything regarding the stored data, that is left up to the provider to handle. But that brings forward the question of how much users can trust the different providers with their data and how much can users trust the providers not to use their data without permission. Other questions that arise are what security threats are targeting the cloud-based storage service and how they can be mitigated concerning the users and the service providers.

1.1 Background

The concept of cloud computing is not new and has been around for some time. It has been a shift in recent years in the adoption of cloud computing where a cost reduction and new business potentials are proposed [6]. Cloud Computing enables universal, connection-based, and on-demand network access to computing resources, applications, servers (both virtual and physical), data storage, and more that are housed at a distant data center run by a third-party cloud service provider. [7, 8]. Comparing cloud computing to traditional on-premise IT infrastructure enables the consumer to lower IT costs by offloading efforts of obtaining, installing, configuring, and maintaining their on-premise infrastructure. The model also improves both the agility it takes to integrate new technologies into an organization and also offers great scalability of already integrated technologies [7].

The cloud computing model has several service models and deployment models associated with it. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) are the three most popular service models. [6, 7, 8]. The cloud service model that this thesis will focus on is the Storage-as-a-Service (StaaS) model where a service provider provides storage that the user can utilize to store different types of data [8, 9]. The different deployment models are for targeting different user areas and user needs. The most common cloud deployment models are public, private, hybrid, and multi-cloud. The privet cloud model is a cloud environment in which all cloud resources and infrastructure is allocated and accessible to only one customer. The public cloud is provided by major cloud service providers like Google, Amazon, and Microsoft and is available to the public or organizations with shared resources. A hybrid cloud is a mix between the private and public deployment mode environments and lets the organization or consumer flexibly choose the optimal cloud for each application. Utilizing multiple clouds from various cloud service providers is known as multi-cloud [7, 8, 10].

It is possible that cloud computing can become more secure than on-premise solutions but it is not guaranteed to be more secure. It depends on how security is approached and achieved. The cloud infrastructure won't protect from all the threats that come from the cyber landscape [11]. There are a lot of threats that target cloud computing in all layers of the computer network and they can be but are not limited to, data breaches, compliance with regulatory mandates, insider threats, the man in the middle attack, phishing attacks, misconfigurations, and more [11, 12, 13]. Due to the nature of cloud computing, consumers need to rely upon and trust the cloud service providers that they are working on securing the cloud service that they are using. The consumer and provider need to do what they can to secure the service; one cannot rely on the other completely.

1.2 Related work

There have been several studies conducted in the field of cloud computing and cloud storage security. One of these studies is from Syed et al. (2020) in "Cloud Storage Security Risks, Practices and Measures: A Review" which focuses on general cloud storage threats and preventive measures [14]. The study derived that cloud computing security is the responsibility of both the vendor and the client. Both parties must uphold their responsibility to maintain an acceptable security level. The study also outlines that achieving end-to-end security is almost impossible due to the highly complex nature of the cloud infrastructure, but securing data and implementing encryption standards where possible can mitigate many risks regarding shared data.

A similar study from Andersson in "En värdering av molntjänsters risker och förebyggande åtgärder" from 2022 evaluates different cloud services risks and mitigation strategies [15]. The study also found that the responsibility of securing the cloud lies both in the vendors and clients. Where the vendors are responsible for data cryptography and the education of their employees while the user is responsible for utilizing the security features that the cloud provider implements. The study shows that one challenge for providers is to present these extra security features such as dual authentication to their users so that the users implement and use them [15]. There is no point in having extra security features if no one is to implement them.

Other studies focus on identifying and providing possible solutions to the threats that are targeting cloud computing. A study by Jangjou and Karim Sohrabi in "A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing " from 2022 did a comprehensive survey on security threats in various network layers in cloud computing [12]. The study outlines different threats/challenges that are targeting both vendors and clients in different network layers. Some of the more important threats that were identified are Distributed Denial of Service (DDoS) attacks, misconfigurations, failure to log events, brute force attacks, main in the middle, account theft, and many more. The report concluded that clients of cloud services had transferred the security

risks and information from their systems onto the cloud environment. In doing so the user has less authority in securing their data and needs to rely more on the provider's security [12].

A similar study from Tabrizchi and Kuchaki Rafsanjani in "A survey on security challenges in cloud computing: issues, threats, and solutions" from 2020 investigated security issues, challenges, and solutions in cloud computing [16]. The study comes to a similar conclusion in that there are a lot of challenges and that the goal of the study was to bring these challenges to light and present possible solutions where possible. Security threats regarding users include identification, authentication, authorization, and access management attacks in various ways. Threats identified targeting the providers are Denial of Service, tampering spoofing, malicious employee, and many more. The study tries to identify future security challenges, and with the emergence of 5G Internet, Internet of Things (IoT) devices, and smart cities where cloud computing will become more important for processing and storing [16].

Different research has been conducted on the security of users associated with using cloud-based applications. A study by Widjaja et al. (2019) in "Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study" investigated users' willingness to upload personal information/data onto personal cloud storage services [17]. From the study findings, they derived that trust, perceived cost, and perceived benefits are the main aspects that affect the users' willingness to upload personal information onto the cloud storage. The study concluded that users were significantly less concerned about security risks and potential data breaches in cases when private information was not sensitive. Moreover, there was a bigger concern when personal or sensitive data were to be uploaded due to potential security threats, thereby lowering the users' willingness to upload that kind of data.

1.3 Problem Formulation

There is a considerable amount of work in cloud computing and cloud storage services regarding security and mitigation strategies. The previous work mostly targets the cloud vendor and what they can do to increase security and what mitigation strategies they can utilize. However, as previously explained in related work both vendors and clients need to do their respective parts to secure the cloud storage service, one cannot do it alone. Cloud service vendors implement security features, and the clients need to utilize those security features to increase the security of the service. There has been little to no research regarding what security features the different cloud storage provider provides and if those security features are utilized by the clients. Because a lot of previous work has targeted vendor-side security, therefore this thesis will investigate client-side security threats, practices, and features. Based on the purpose of this thesis these three research questions have been formulated:

- RQ1: What are the current security threats targeting clients in cloud storage services?
- RQ2: What are the current security practices that clients implement when using cloud storage services?
- RQ3: What security features do popular cloud storage services provide to their clients?

1.4 Motivation

Breaches on cloud-based systems happen regularly. In 2022 the digital scheduling platform FlexBooker experienced a data breach where the sensitive information of 3.7 million users was compromised. The attackers infiltrated the company's AWS (Amazon Web Services) servers. The data included in the breach was personal details such as names, email addresses, phone numbers, password hashes, and incomplete credit card information. The perpetrators later sold this information on several underground hacker forums [18].

This thesis will advance cloud storage service security with a focus on client security threats, practices, and security features. The results will address two very important areas, client security practices and security threats and mitigation features provided by the cloud storage service providers. These two parts are essential to better understand clients' security practices and what type of features the provider provides its clients to increase their security while utilizing their service. From a societal perspective, it will give clients knowledge about the different security features that cloud storage providers provide, and from an industrial perspective, it will grant insight into what implemented security features the clients are utilizing. Giving valuable information about what security features could need a change to increase its usage among the clients.

1.5 Results

The paper presents cloud storage client target security threats, users' security practices, and a comparative analysis regarding security features that are provided by cloud storage providers. To answer those three questions, three methods have been selected and will be used as follows.

In the literature review, we will search and present common security threats that are targeting clients of cloud storage services. In doing so we hope that we can bring light to client threats making it more known that all security can not only be mitigated by the cloud storage provider and that some threats need to be addressed by the clients themself.

The survey will consist of several questions that the participants will answer. The questions will target different user security threats that are related to clients of cloud storage services. The questions will be targeted toward password management, the man in the middle, fishing attacks, and overall threat handling. By letting participants answer

these questions we hope that we can get an overview of the participant's security practices when it comes to the usage of cloud storage services.

Lastly, the comparative analysis will be conducted to compare four large cloud storage providers and compare the security features that they provide to their clients. In doing so we hope that we can see what the different cloud providers offer to their clients and provide a good overview to potential clients and provide them with information regarding the different cloud storage providers' security features.

1.6 Scope/Limitation

There is a vast amount of different cloud storage service providers available on the market and there are even more threats that are targeting the users of these services. It is impossible to assess all cloud storage providers and all the threats in this thesis. It is therefore important to limit the scope of this thesis to a realistic and achievable one. This thesis will only investigate the four largest cloud storage service providers on the market at the time of writing. The four cloud services that will be investigated are Google Drive, Dropbox, Apple iCloud Drive, and Microsoft OneDrive. These providers have been selected based on their widespread adoption and popularity among the population. The four cloud storage providers provide an easy way of creating an account and give their users a small storage capacity without the need to pay. This is a great advantage and an impactful feature because the user can try out the storage service without a paywall and if the user liked the service, the user could then increase the storage capacity. The four storage services will be compared based on the security features that they provide to their clients. Another limitation this thesis will do is to narrow down the threats that will be brought up in this work. There is a large number of threats that are targeting users of cloud storage services and it would be important to cover them all. Therefore, this thesis will focus on the threats that are deemed relevant by the authors.

1.7 Target group

The target group for this project comprises individuals who use cloud storage solutions as part of their personal life. This study aims to understand users' security practices while using cloud storage services. The study also aims to provide security threats that target users and compare the four most popular cloud storage services' security options that they provide to their users. The findings of this study will be useful to individuals on how they can utilize extra security features and thereby increase their security while using a cloud storage service. The study will also provide a comparison of the four most popular cloud storage services and their different security options and features. This can be good for users when they are considering which cloud provider storage service they should choose.

1.8 Outline

The structure of this report is as follows. In Chapter 2 we discuss the methodology that will be used in this thesis to answer the research question. The chapter will also discuss reliability, validity, and ethical consideration when it comes to the methods that have been selected for this work. Chapter 3 provides the theoretical background and discusses the knowledge gap and answers the first research question on what current threats are targeting clients in cloud storage services. Chapter 4 will focus on describing how the survey was conducted and how the comparative analysis of the 4 cloud storage providers where done and what we compare. In Chapter 5 the result of both the survey and the comparative analysis will be displayed. Chapters 6 and 7 will focus on analyzing and discussing the result that has been presented in Chapter 5. Lastly, in chapter 8 we will discuss the conclusion of our thesis work and also outline future work that can be done in the field of investigation.

2 Method

This chapter will present the methods used to conduct this thesis. The reader will be given a thorough understanding of each method's objective and use of this study by way of detailed examples. This essay clarifies worries about cloud service vulnerabilities through a survey, literature review, and comparative analysis. While the literature review discusses possible and actual actions as well as current risks and concerns surrounding cloud services, the survey will focus on users' security practices. The comparative analysis compares the various cloud service providers for the user's account's security level.

2.1 Research Project

This thesis aims to investigate the challenges related to security threats in cloud services by utilizing three methods: a survey, literature review, and comparative analysis. The survey will examine user perceptions of security, while the literature review will analyze current threats and risks associated with cloud services, as well as potential and existing security measures. The comparative analysis will compare different options available for securing user accounts in cloud services. By utilizing these methods, this study aims to provide a comprehensive understanding of the security issues associated with cloud services and propose effective solutions for mitigating these threats.

2.2 Research methods

The research plan includes several research methods that have been selected to address our research questions (RQs). Furthermore, to provide valuable insights into the users' security practices and challenges associated with cloud storage services.

Firstly, we intend to conduct a literature review (comprehensive literature study) to address RQ1. With the use of this technique, we can better grasp the issues surrounding user security in cloud computing. The literature review technique was chosen because it enables us to methodically assess already published research and studies in the area and to give a more thorough picture of the state of the subject today. By doing a literature study, we want to better understand the security problems that cloud computing now faces and pinpoint potential solutions that consumers might be able to apply. We can make sure that our study is well-informed, and current, and helps to fill the identified research gap by analyzing the literature [19].

In addition, We will conduct a survey using questionnaires to gain insights into users' current practices toward security while using cloud storage services. We have chosen a survey as the preferred method because it offers a convenient and efficient way to gather a large and diverse dataset from a significant number of participants, which will enhance the reliability and generalizability of our findings. Additionally, the survey method allows for efficient data collection, which increases our responses within the time constraints of

our research. By aligning the survey questions with RQ2, We want to find out what users' reaction is when security breaches happen, such as database leaks. This method will help to obtain concrete and measurable data to analyze and draw meaningful conclusions from, instead of relying solely on speculative assumptions. The survey will provide valuable insights into user security practices and preferences in cloud storage services [20].

Furthermore, we will conduct a comparative analysis of the selected cloud storage services to address RQ3. This approach will provide us with a better understanding of the services' features and how to implement security measures for cloud storage services effectively. We have chosen comparative analysis because of it allows us to compare and contrast the security capabilities of the services. The analysis will involve a manual review of the services' security features and password requirements. By conducting this analysis, Our aim is to identify the strengths and weaknesses of each service and assist users in making informed decisions regarding their data protection. This method will complement the other research methods and ensure that we develop a comprehensive understanding of the security challenges associated with cloud storage services.

The research workflow throughout this thesis can be seen illustrated in figure 2.1 and is as follows. The research will start with a comprehensive literature review, where the goal is to answer the first research questions and give an insight into the field of study. The insight gained from the literature review will be used to produce the questions that will be used in the survey. The conducted survey will be used to gather data on users' security practices while using a cloud storage service. The conducted survey and its questions will first need to be approved by this thesis works supervisor before it will be sent out to respondents to answer. The collected data from the survey will be analyzed and will help to answer the second research question. While the survey is out and gathering respondents, a comparative analysis will be conducted where the goal is to answer the third research question. Based on the information that has been collected during the literature review, a number of points will be made as to what to compare the different cloud storage services against. When that is done and the survey has been brought down, this thesis research is completed.

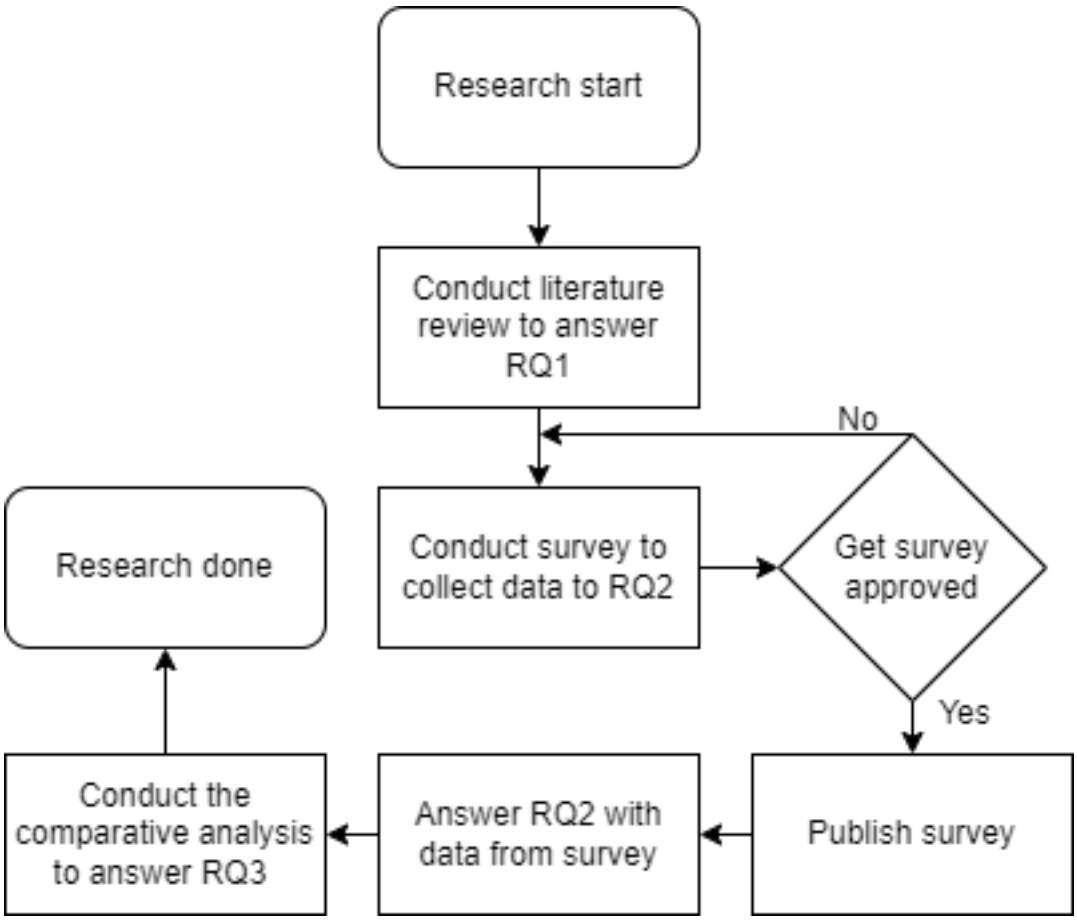

Figure 2.1: Chart of the workflow in this thesis work of answering the research questions

The methods selected for this thesis work were selected based on the research question that it is meant to answer and how effective they are. The literature review was selected because it is a good way of getting insight into the field without taking up to much time. Another method that could have been selected would be to do a systematic literature review. The problem with a systematic literature review is that it takes a lot more time and effort to complete. If a systematic literature review were to be chosen, the survey and comparative analysis would have to be discarded and the research questions need to be reformulated to fit into the systematic literature review.

There are a number of ways in collecting data regarding user usage of a service. The most popular method is either to do an interview or to conduct a survey. A survey was chosen because of how the research question was formulated. It demands a large number of respondents to be able to generalize the answers that are gathered. In this case, it would be hard to do interviews due to the large number of interviews that needs to be done. If the research question were to be reformulated to where a large number of respondents are not needed, interviews would be more feasible.

The method used to compare the different features that different cloud storage providers have was done by conducting a comparative analysis. This method allows compressions between different items, in this case, cloud storage service security features. Dou to how

the research question is formulated there are no other suitable methods that can be used to compare and discuss differences and similarities between the different services.

2.3 Reliability and Validity

Multiple sources of data that can be cross-referenced and independently verified are provided by the use of surveys, literature reviews, and comparative analyses. The survey will be useful in collecting data from a number of participants, but there might be biases in the participants, which is not easy to detect. Therefore, we have to assume that the participants answer truthfully. The review of the literature will offer information on recent studies and publications on cloud computing security. choosing articles as the latest from 2018 we can be sure to get reliable data. The authors have no notable biases within this subject. The comparative analysis will allow us to pinpoint the benefits and drawbacks of the security of each service and offer suggestions for improving security. The authors have no notable favorite cloud storage services and will evaluate each chosen service to its full extent and later compare the results side by side.

An understanding of the security issues related to cloud storage services will be provided by the combination of the survey, literature review, and comparative analysis. By presenting various viewpoints on the research topic, the use of multiple research methods can increase the validity of the study. The survey questions will gather information about user attitudes and behaviors that will help with this thesis's questions. Before the survey is published a group of persons will review and evaluate the survey. The literature review and comparative analysis make sure the conclusions are based on reliable research and accepted business standards.

2.4 Ethical considerations

Overall, it's important to ensure ethical considerations are followed when conducting any type of research or analysis. For a literature review, it's crucial to avoid purposely misinforming the data gathered through sources. Additionally, it's essential to ensure the data gathered is fact-checked or peer-reviewed articles should be our main source of information. Any security measures taken should also be valid and reliable.

When conducting a survey, it's vital to follow the guidelines of GDPR. This includes not collecting any personally identifiable information from participants such as their names or contact information. Using a secure tool like Google Forms can help ensure data breaches are avoided. Furthermore, it is important to note that our research did not collect any sensitive information that could potentially enable malicious actors to link participants. The data gathered for this report does not pose a significant risk of being exploited by malicious individuals to compromise the privacy or security of users or providers. Therefore, the likelihood of malicious actors using the information in this report for breaching is minimal.

In terms of the comparative analysis of selected cloud storage services, there may not be any specific ethical considerations. However, it's still important to ensure that any information used is accurate and reliable to ensure unbiased conclusions. Handmade tables can be used to present results clearly and concisely.

3 Theoretical Background

This chapter aims to provide a clear understanding of Cloud Computing and Cloud Storage Services. Additionally, this chapter will discuss security risks associated with Cloud Storage Services that users will face and will thereby answer the first research question. A literature review has been conducted where the digital databases IEEE Xplore and Scopus were used to find and evaluate papers within the research area. To be able to filter out irrelevant papers a number of inclusion and exclusion criteria were created. The inclusion criteria for the papers are that they need to be in the field of Cloud Storage and need to be published between the years 2018 to 2023. The exclusion criteria for the papers are that the study was published before 2018, the study was published in a langue other than English, or the study is not accessible through Linnaeus University. Searching for papers a set of keywords in combination with the advanced search that the two sources provide. The keywords used on both digital databases are “Challenges” and “Threats”. The keywords were chosen based on the first research question and what it requires to be able to answer the research question. The research question aims to assess security threats/challenges that are targeting users. It was hard to find papers only covering user threats and challenges, resulting in a rather small sample size of studies. Therefore a broader approach was taken to not only look at studies that only cover user-specific threats and challenges but rather look at studies that investigate threats and challenges in the cloud storage environment and then pick out user-specific threats from the identified papers. Below is a table showing how many articles each keyword search resulted in for each digital database. See table 3.1 and table 3.2 for the number of papers found for each keyword in both digital libraries.

Table 3.1: Shows the number of papers found for each keyword in the digital library Scopus.

Scopus		
Keyword	Search String	Papers
Threats	(TITLE (("Cloud Storage*" OR "Storage as a Service*" OR "STaaS*") AND ("Threats*")) OR KEY (("Cloud Storage*" OR "Storage as a Service*" OR "STaaS*") AND ("Threats*"))) AND (LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT-TO (LANGUAGE , "English"))	53
Challenges	(TITLE (("Cloud Storage*" OR "Storage as a Service*" OR "STaaS*") AND ("Challenges*")) OR KEY (("Cloud Storage*" OR "Storage as a Service*" OR "STaaS*") AND ("Challenges*"))) AND (LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT-TO (LANGUAGE , "English"))	86

Table 3.2: Shows the number of papers found for each keyword in the digital library IEEE Xplore.

IEEE Xplore		
Keyword	Search String	Papers
Threats	("All Metadata":"Cloud Storage*" OR "All Metadata":"Storage as a Service*" OR "All Metadata":"STaaS*") AND ("All Metadata":"Challenges*") AND ("All Metadata":"Security*")	64
Challenges	("All Metadata":"Cloud Storage*" OR "All Metadata":"Storage as a Service*" OR "All Metadata":"STaaS*") AND ("All Metadata":"Challenges*")	186

3.1 Cloud Computing

The definition of cloud computing is best described by NIST "Cloud computing is 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." [8]

There are many different components that make up the architecture of cloud computing, including servers, infrastructure, applications, and platforms. The entire cloud ecosystem is coordinated by significant components known as cloud actors. A set of cloud actors, their roles, and activities are described in a standard reference architecture that the National Institute of Standards and Technology (NIST) has established [8, 21]. Cloud Consumer, Cloud Provider, Cloud Carrier, Cloud Broker, and Cloud Auditor are the five categories into which these actors are divided. Each of these actors is an individual or an organization that performs particular tasks related to cloud computing and has a defined function. The following list summarizes each actor's main duties:

- The cloud provider is in charge of allocating, orchestrating, managing, and providing services to interested parties while adhering to the SLAs set forth with other actors (in particular the Cloud Consumer).
- An individual, a group of individuals, a small- or medium-sized business, a multinational corporation, or a government can all be considered a cloud consumer.
- In accordance with established SLAs, a cloud carrier (also known as a network provider) acts as a middleman to provide connectivity and transport of cloud services from cloud providers to cloud consumers.
- An intermediary party known as a cloud broker negotiates the contract between a cloud provider and a cloud consumer. It might provide fresh services that make managing Cloud Consumers easier.
- To ensure that suppliers are adhering to their SLAs, Cloud Auditor is in charge of auditing the performance and security of Cloud Computing services provided by Cloud Provider, Cloud Carrier, and Cloud Broker.

3.1.1 Computing deployment models

The different ways in which users can access cloud services are referred to as cloud computing deployment models. How the services are deployed, offered, and consumed, as well as the degree of customer confidence in third-party providers, define these models. Public, private, community and hybrid clouds are the four main cloud computing deployment models [22, 23].

The public cloud model is a well-known cloud service. Web applications, file sharing, and non-confidential data storage frequently use this kind of cloud. For collaborative projects and software development, public clouds are advised. The entire hardware required to run a public cloud is owned and managed by the service provider. The devices are kept by vendors in sizable data centers. For testing and development, the public cloud delivery model is crucial.

Private cloud deployment model is also called the internal or corporate model. An organization's private cloud is its property. The system is managed and under the organization's command. A private cloud server can be hosted by a third party (like a service provider, for instance. The majority of businesses opt to keep the hardware in their neighborhood data center. From there, everything can be supervised and managed by a team within.

Community Cloud is a cloud service that offers services to a group of people or businesses who have similar interests or problems. The missions, governance, security standards, and policies of the organizations using this cloud service are similar. Cloud services may be housed at one provider, at the location of the peer organization, on the premises of the consumer organization, or a combination of these locations. Although the actual cloud could technically be a VPC, private, or hybrid cloud model, the term "community cloud" is frequently used in marketing to explain the service's target customers.

Hybrid clouds combine public clouds with private clouds. They are made to interact seamlessly between the two platforms and to move data and applications between them. It is the ideal solution for a company or organization that requires a little bit of both, which typically depends on the industry and size. Essentially, a hybrid cloud begins as a private cloud and extends the integration to use one or more public cloud services. When businesses have sensitive data that cannot be stored in the cloud or are subject to regulations that demand data protection, storage, and other requirements, this deployment model makes sense.

3.1.2 SaaS, PaaS, and IaaS

Software as a Service (SaaS) is a cloud computing model where users can access applications provided by a third-party vendor through a thin client interface, such as a web browser. Users communicate with the application via the Internet using a local client, which the vendor hosts on their servers. Users are not required to manage or keep an eye on the network, operating systems, storage, and servers that make up the underlying infrastructure[24].

Platform as a Service(PaaS) is a cloud computing model in which consumers can use a shared platform to configure, deploy, test, and develop application software without the need to maintain servers, hardware, and storage. To operate the application, the cloud vendor offers a pre-installed operating system.

Customers have control over the application, including the ability to use the programming languages and tools supplied by the provider to deploy their own developed or purchased applications or software. The parameters of the hosting environment and application deployment may be under the client's control, but the cloud infrastructure is not [24, 25].

Infrastructure as a Service (IaaS) is a cloud computing model where consumers can deploy their applications and systems using a shared infrastructure, but they cannot control the underlying infrastructure. The consumer can deploy programs that may include operating systems and other applications by utilizing various computing resources, including processing, storage, and networks. By predetermined specifications, they have control over the deployment of operating systems, storage, and applications as well as particular networking components. However, the consumer cannot manage or control the cloud infrastructure itself. IaaS offers virtualized computing resources via the Internet through platforms like Google Compute Engine (GCE), Microsoft Azure, and Amazon Web Services (AWS). These services are provided by cloud service providers (CSPs) using virtual machines [24, 25].

3.1.3 Storage As a Service (STAAS)

Storage As a Service also known as STaaS, is a cloud storage option that Cloud Service Providers (CSPs) sell on a subscription basis that includes the most basic access techniques. The cloud can be used for multimedia storage, data repositories, data backup and recovery, and disaster recovery by businesses, small and medium-sized businesses, home offices, and individual users. [26].

Organizations may efficiently manage their storage capacity and workloads with STaaS, which eliminates the need to spend extra money on staff time or on storage gear or software. Organizations or individual users can streamline their operations by subscribing to storage services, allowing them to instantly access and use a vendor's infrastructure [27].

STaaS solutions can be rented based on the amount of storage required, while others are based on service level agreement (SLA). SLAs are essential in defining and laying out the conditions for using data storage, such as read/write access rates and uptime. The choice of storage is typically influenced by how frequently you access the data. Warm or hot data is accessed regularly, while cold data is designed for infrequently accessed material largely left untouched [26]. StaaS offers a way to buy and remotely manage storage across multiple configurations, such as on-premises, co-located, or hybrid cloud environments, in the context of cloud computing. Similar to other cloud services, organizations purchase storage by deciding on the necessary computation, networking, and storage capacity as well as their encryption and security standards [27].

Since data center operations related to storage are frequently among the most expensive, STaaS is a desirable choice for many businesses. It takes more work from the IT

team to manage the market's constantly expanding stream of data. Organizations may centralize their operations, enhance cost control, and have access to flexible capacity that dynamically adjusts to their demands without causing downtime by subscribing to StaaS [27].

The management of data access inside an organization and choosing the proper permission levels, such as read-only or read-write access, are the main security concerns for STaaS users. It is critical to keep in mind that CSPs do not manage access to the devices of their clients. Therefore, to avoid vulnerabilities at the access points, it is essential to be proactive in protecting against attacks like email phishing schemes. Additional layers of security can be added by putting strong security measures into place, such as two-factor authentication, secure passwords, and adherence to other best practices [26].

The enterprise can benefit from the following [28]: [28]:

1. **Cost savings:** Reduced expenses related to personnel, hardware, and physical storage space.

2. **Improved disaster recovery:** Enhanced recovery measures due to data being stored in multiple locations.

3. **Scalability:** Users pay only for the resources they use with most public cloud services.

4. **Automatic syncing:** Files are seamlessly synced across multiple devices.

5. **Security:**Security in cloud storage has its advantages and disadvantages, with different methods varying by vendor. One common approach is encrypting data during transmission or while at rest. However, there are some drawbacks to Storage as a Service (STaaS):

Common disadvantages of STaaS include the following:

1. **Security risks:** Security risks: When transferring sensitive data to the cloud, it is crucial to carefully select a trusted service provider to mitigate potential security risks. This ensures that data remains protected and confidential throughout its storage and retrieval process.

2. **Potential high storage costs:** It's important to be mindful of exceeding bandwidth limitations in cloud storage, as it can lead to increased costs. Organizations should consider their storage needs and plan accordingly to avoid unexpected expenses related to storage usage.

3. **Possibility of downtime:** Vendor downtime may render services unavailable, causing issues for mission-critical data.

4. **Limited customization:** Cloud storage relies on infrastructure owned and managed by the service provider, which may restrict the level of customization available to users. This can limit the ability to tailor storage configurations and features according to specific needs or preferences.

5. **Vendor lock-in risks:** Once an organization adopts a particular cloud storage service, migrating to a different provider can be challenging. The integration of data, applications, and processes with a specific vendor's platform may create dependencies that make it difficult to switch providers without significant effort and potential disruptions.

3.2 Cloud Service Considerations for Client Engagement

The following subsections delve into important considerations for cloud service providers to enhance client engagement. These considerations include the service-level agreement (SLA), client experience, and client authentication. These aspects play a significant role in managing customer expectations, delivering personalized solutions, and ensuring the security of sensitive data in cloud computing environments.

3.2.1 Service-level agreement (SLA)

An SLA is a contract that specifies the service performance requirements between a service provider and a client. It cannot ensure a specific service outcome, but it can manage customer expectations and establish provider responsibility. It typically includes service goals, and each party's obligations, but also specific benchmarks for performance, availability, and response times [16].

3.2.2 Client experience

Customers anticipate that service providers will comprehend their particular needs, specific situations, and difficulties in daily life. In order to give superior services, providers must ascertain the wants of their clients and present specialized solutions. In the world of cloud computing, the customer experience is essential because it enables businesses to offer goods and services that are consistent with what customers value [16].

3.2.3 Client authentication

An essential security mechanism to stop unwanted access to private or sensitive data is authentication and to ensure that system performance is not jeopardized [29, 30]. It requires both the server and the client to confirm the accuracy of the data sent back and forth. Client devices are typically considered a weak link in the security chain since user credentials are regularly stolen, and password protection is universally acknowledged as

essential. Attackers who attempt to pass as a network server or client can take advantage of flaws in client-server communication protocols through impersonation attacks. To guarantee the integrity and confidentiality of the communication contents and prevent unauthorized access to the system's data, a secure protocol is required [30].

3.2.4 Client-centric privacy

These days, cloud vulnerabilities are most noticeable when data privacy is violated, causing data leakage. This problem, which compromises customer privacy, is mostly caused by data processing by cloud providers. Since customers have no control over how their data is processed, this issue is a major barrier to the adoption of cloud services. They are not aware of where, how, or why their data is being used. Without the user's consent, the service provider may disclose sensitive information to unapproved parties, resulting in data leakage and privacy loss. A client-centric solution that gives users control over their submitted data is therefore required to resolve this issue. To handle the potential problems with security, privacy, trust, and customer relationship management, it is crucial to take a client-centric strategy [16].

3.2.5 User Awareness strategy

When computer network problems occur in a cloud computing environment, users may be directly impacted. Increasing user awareness of preventative actions is essential to preventing user data from being stolen, corrupted, or otherwise compromised. Users' understanding of computer security can be gradually increased using techniques like training, advertising, and different instructional approaches. Raising this awareness will support stable computer operation, reduce the likelihood of numerous security risks, and ensure correct operation. [31]

3.3 Threats Against Cloud Storage Users

This section will present threats in cloud storage services that are targeting users. The threats are derived from the conducted literature review.

3.3.1 Account Hijacking

Account Hijacking is a serious issue where an attacker can take control of a user's account and change, modify, and edit content and account details. An attacker can take control of an account and change passwords and recover emails looking out the user from the account, making it harder to recover the account [32]. Account hijacking is made possible by several underlying attack strategies such as phishing attacks, brute force attacks, Server-side request forgery, Infected Browsers, and many more [33]. All the attacks have

a similar goal of stealing account authentication credentials to be able to log in to the account and possibly steal or modify data. Phishing attacks use social engineering to trick users into giving the attacker login credentials. While a brute force attack heavily relies on cracking passwords to get access to the account. Therefore, users need to be aware of these kinds of threats and how they can be mitigated to keep their accounts secure.

3.3.2 Brute Force Attack

A brute-force attack is a common attack technique used to break encryption keys, API keys, passwords, PIN codes, login credentials, and more to gain access to user accounts or networks. The method involves forcefully "guessing" a password until the attacker gets the password right and gains access to the account or network [34, 35]. A brute-force attack is exhausting work and is not implementing any intellectual strategies to crack the password. The method involves an application that tests all combinations of possible characters in a sequence until the right password has been found. The time it takes to crack a password can vary greatly depending on how "strong" the password is. A bad password can be cracked in just a few seconds while a strong password may take hours or days [36]. Even though the cracking time can vary greatly, it is still a simple method but it has a high success rate, is still widely adopted, and remains a popular tactic [34].

Several different types of brute-force attack methods can be utilized when cracking passwords. Some of the methods are simple brute force attacks, dictionary attacks, and more [34, 35]. The simple brute force attack is when the attacker guesses login credentials manually without the help of an application, this is done by typical standard passwords and PIN codes or by doing minimal social engineering to get a sense of the user's password. This attack is still successful because users still use bad passwords such as "password12345" and "123456" or the users have bad password practices [34]. Bad password practices refer to once-bad habits when it comes to password management such as reusing old passwords, using known weak or bad passwords, using short passwords, and many more [37]. A dictionary attack is an attack where the attacker uses a pre-defined list or lists of potential passwords that are then tested. The directory lists can be created in different ways. The passwords in the dictionary lists can be taken from a data breach or consist of the most common passwords or a combination of both. This attack is time-consuming and has a low success rate compared to other brute-force attacks of the same caliber [38]. However, the directory attack is still faster than the manual simple brute-force attack.

3.3.3 Phishing Attacks

Phishing attacks are a type of social engineering attack that is used to wrongfully acquire user information, including authentication codes, credit card numbers, and other sensitive data. The attacker tries to imitate, mimic, or masquerade as a trusted organization or entity

and devices the victim into opening and interacting with an email, instant message, or text message. The victim is then further tricked into clicking malicious links that can either download and install malware or further trick the victim and steal user authentication credentials [39].

There are several types of phishing attacks and there are several different techniques that can be utilized. Spear phishing, whaling, and clone phishing are just a few examples of different phishing attack types [40, 41]. Spear phishing is a phishing attack that is one of the more popular and is targeted toward individuals instead of a wider target group. Because the attack is targeted toward a specific individual, it can contain personal information, making it more authentic. Much like spear phishing, whaling is also a targeted attack that targets CEOs or other privileged users within a company or business [40, 41]. Clone phishing is an attack that tries to clone a previously legitimate email and modify the links or attached files to trick the victim into opening a malicious file or website. This attack is successful because it seems to come from a trusted source and can thereby exploit the trust to make the victim take action [40].

Most phishing attacks have a similar structure to them and they tend to use emotions to get the victims to open attachments or click provided links. Emotions that can be used are fear, urgency, greed, or curiosity. The attacks are meant to look as similar as possible and are designed to come from the trusted source that they claim they are from. Cybercriminals are often innovative and are coming up with more sophisticated attacks and it can be hard for regular people to keep up with the constant innovation. It only takes one successful phishing attack to steal the victim's authentication credentials or compromise the victim's network or computer [41].

3.3.4 Infected Browsers

An infected browser is a web browser that has been hijacked or compromised with a malware application that changes and modifies how the browser works without the user's permission. An infected browser can also be referred to as a browser redirect virus because it redirects users to malicious websites or other insecure websites [42]. The goal of an infected browser is to force users to visit certain websites so that the hijacker can capitalize on high advertisement revenue and thereby finance other illegal activities. An infected browser is not only limited to redirecting users but can also contain spyware or ransomware [43]. Spyware enables the attacker to obtain sensitive information such as a user's banking information, credit card numbers, account authentication credentials, and user browsing behavior. The gathered information can then, later on, be sold to third parties or saved for later use. Ransomware is a type of malware that encrypts data in the victim's computer and to get it back the victim normally needs to pay the attacker a ransom to get the encrypted data back [43].

A browser can be infected in several ways including shareware, freeware, or advertis-

ing support applications that can be deployed through the installation of web browser toolbars or add-ons [42]. The malicious applications are often unintentionally downloaded by the user or the user is tricked/fooled into downloading the malicious application. When the application is installed, malicious code is embedded and starts to alter the user's web browser. The severity of the infection varies from attacker to attacker depending on their end goal. Some attackers may only change small things that are more annoying than dangerous for the user while others may change a lot, making it more dangerous for the users [43].

3.3.5 Man-In-The-Middle Attack

The Man-In-The-Middle (MITM) assault is a sort of cyber attack in which the attacker inserts himself in the middle of two parties having an online communication. The attacker secretly intercepts and relays internet packages between the two parties. For the attack to be successful the two parties must believe that they are communicating directly with one another and that no one is intercepting them [44, 45]. The MITM is a type of eavesdropping in which the goal is to steal personal information, such as authentication credentials, credit card details, or similar information from applications where login is required. The stolen information can then be used to commit identity theft or account theft among other illegal activities [45].

The Main-In-The-Middle Attack consists of two phases, one interception phase, and one decryption phase. The first step is intercepting the user's network traffic before reaching the targeted destination. There are several ways to intercept network traffic, one passive way is to set up a malicious free WiFi hotspot where network traffic can be monitored [45]. There are more active ways to conduct the MITM attack that involve spoofing or hijacking different network elements such as Internet Protocol spoofing, and Domain Name System spoofing among others [44, 45]. After the intersection phase, any traffic that uses an encrypted channel needs to be decrypted to obtain the information communicated between the parties. This needs to be done in a way that does not alert the involved parties. There are several ways this can be achieved such as HTTPS spoofing, SSL hijacking, or stripping among others [44, 45].

3.3.6 Denial of Service

A Distributed denial of service (DDoS) attack or Denial of Service (DoS) attack is an attack launched by malicious actors and aims to render the target resource unavailable to the intended user [46]. Resources that could be targeted are computer systems, networks, services, or other IT resources [47]. The difference between DoS and DDoS is the number of resources that are used to launch the attack. A DoS attack uses only one computer to launch the attack while a DDoS uses several different distributed computers to launch a simultaneous attack on the target. The are several ways in which a DoS or DDoS attack

can be carried out. Typically the attacker floods and overwhelms the target resource with enough network traffic or requests until the resource either crash or are no longer able to handle normal user traffic. When this point has been reached the resources are no longer able to provide the service to its intended users and thereby resulting in a denial of service [46, 47]. Restarting a crashed system usually fixes an attack that crashes the system, but a flooding attack is harder to recover from and DDoS are even harder to recover from due to several sources that the attack is launched from [47].

3.3.7 External Sharing of Data

The cloud is designed to make data sharing easier between parties. Plenty of cloud storage providers have the option to invite collaborators through email or direct sharing of a link that enables anyone to access the shared resource. This can be a great asset when it comes to shared resources, but it also comes with a great cloud storage security risk [32]. The usage of linked-based invitations is a popular option when inviting collaborators since it is easier than manually inviting each collaborator separately. But this comes with a great cost of lack of access control to the shared resource. The shared link can further be forwarded to a third party unintentionally or intentionally and thereby compromising the shared resource and granting unauthorized access to third parties. The problem with losing access control to the resource is that it makes it hard to know who has access and even harder to revoke access to the resource [32]. This is a huge security challenge that users need to be aware of when sharing their cloud resources with collaborators.

3.3.8 Summary

Many of the threats that have been identified and talked about in this report have in some way or form a connection to user account management. Some of the threats identified are not only limited to cloud storage accounts but to all types of accounts that the user can create on the internet. Phishing attacks, Infected browsers, Man-In-The-Middle attacks, and brute force attacks are all threats that are directly targeting user accounts. The attacks are aimed at users' authentication credentials such as username and password and the main difference is how the attack is performed. The brute force attack is the only attack that is actively trying to crack a user's password to get access to the account. The other attacks are more passively trying to catch user authentication credentials by different means either in transit, by spyware, or by social engineering. Therefore, users must have a basic knowledge and understanding of how they can protect their accounts from these kinds of threats. Basic account and password management and best practice is something that would benefit all users and make the service more secure to use.

4 Research project – Implementation

This chapter will go through the research project implementation regarding the survey and the comparative analysis. The survey's purpose, arrangement, and question selection will be discussed. Furthermore, the chapter will also discuss the implementation of the comparative analysis, its purpose, and what aspects will be compared. The literature review laid the groundwork for constructing the survey and the comparison analysis. Based on the threats that have been identified by the literature review, a survey has been conducted to get the respondent's security practices regarding some of the identified threats. The comparative analysis will also take the identified threats from the literature review as the foundation for what to look for when assessing the different providers. The result from the comparative analysis will give an insight into what security features different providers provide to their users.

4.1 Survey overview

The survey included in this thesis contains eight security-related questions aimed at assessing the security practices of users who employ Cloud Storage Services (STaaS). The objective of the survey is to enhance the findings of RQ1 and RQ3, and to provide insights into RQ2. To ensure the survey's validity and reliability, we restricted its dissemination to forums accessible only to students and teachers of the computer science programs at Linnaeus University. This measure was adopted to prevent unauthorized persons from tampering with the survey results. However, it also resulted in a reduced response rate and biased population.

The questions in the survey are designed to indirectly ask the participants about the security practices employed by participants. These questions are informed by the efficacy of various techniques that can help mitigate diverse security threats. Each question has multiple alternatives and in some cases an "Other" field where the participant can write other alternatives not mentioned earlier. As the focus of our research is on security practices, we have not included questions about participants' gender, age, or computer science knowledge, as we deemed this information irrelevant to our research objectives. Additionally, we recognize that such personal questions can make some participants uncomfortable, so we have refrained from including them.

The survey is conducted using Google Forms, a free form-building tool provided by Google. This tool was chosen for its user-friendly interface for both form creators and respondents. The statistics and responses for each question are detailed, and the answers can be exported to Microsoft Excel, which is significant for presenting the results chapter. It's worth mentioning that the answers from Google Forms are stored securely in the respondent's Google account and can only be accessed by the creator of the form who has been granted permission to view and analyze the responses. This ensures that the data

collected remains private and confidential. See Figure 4.2 and 4.3 for an example question and for an example answer distribution.

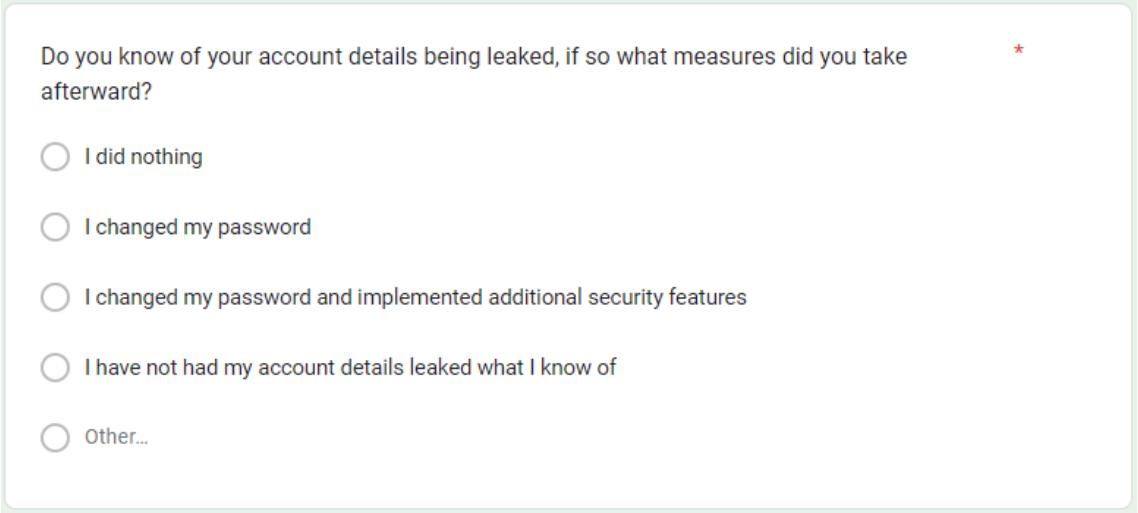

Figure 4.2: An example of a survey question and respondent user interface representation

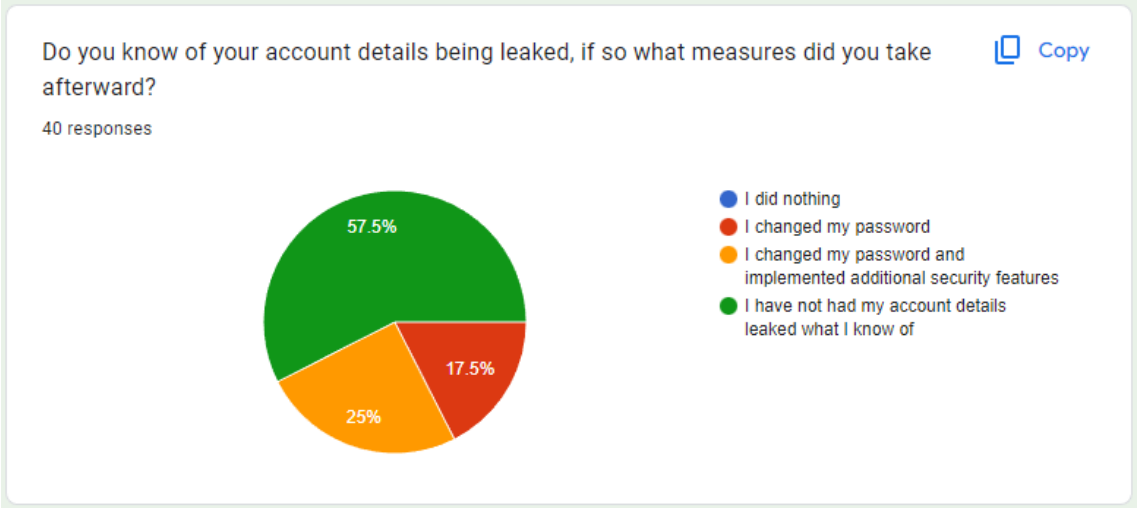

Figure 4.3: An example of respondents' answer distribution for each question

4.1.1 Survey Design

Our aim with the service is to gather information about users' practices when using cloud storage. It is therefore important to get as many respondents as possible to be able to draw a general conclusion about user practices. We tried to keep the total number of questions as low as possible, ideally around 10, to make the survey more attractive and simpler for participants to complete. This was accomplished by carefully selecting the questions, making sure they weren't extremely complex or repetitive. Because of this, we chose to stop the survey at eight questions, certain that this would provide us with the data we needed.

The only question type in this survey is a multiple-choice question. This is as a result of all the benefits it provides. One of the main benefits of multiple-choice questions is the capability of standardizing responses. Giving respondents a choice of responses reduces response variability and makes it simpler to compare and analyze the results.

multiple-choice questions require less time to complete and are easier to administer than Open-ended questions. As a result, the survey is quicker to complete and more attractive to respondents.

Multiple-choice tests can also lessen the impact of response bias. Participants are less likely to be swayed by issues like social desirability bias or a lack of subject understanding when response options are provided.

Compared to surveys with open-ended questions, multiple-choice questions can raise the response rate. This increases the sample size and the data's representativeness because more people are likely to complete the survey.

In specific circumstances, a multiple-choice question might have an "Other" section to let respondents choose a different answer that wasn't presented in the first few options. Usually, this option is included to allow respondents to communicate a significant response that the survey's designer may have missed. It might be possible to combine the response with an already existing choice if it is comparable to one. In general, adding a "Other" section can improve the precision and thoroughness of the information gathered through the survey [20].

4.2 Comparative Analysis

The comparative analysis assesses the security features of the top four most common and recognized storage-as-a-service providers (Google Drive, Dropbox, Apple iCloud Drive, and Microsoft OneDrive). The goal is to make a comprehensive comparison between the different security features that are provided by the different providers to their users. The comparison will be done as followed, we will create a new account and the four cloud storage services. While the account is created we will look at what password rules the cloud provider has when we create our password. We will also look at what we get for recommendations for extra security features like two-factor authentication and other security features. Once the account is created, we will look into account security and see what extra security features they have. This will bone to the four providers and we will then present our findings in this thesis. The result from this comparison will help future users make an informed decision on what provider to choose based on the security they offer.

4.2.1 What will be compared

The comparative analysis will consist of several questions that have been derived from the conducted literature review. The questions will be tested on all four service providers'

cloud storage and then compared to one another. The questions will cover different aspects of user security and management such as password security, account management, and security features. Below is a list of things that will be tested:

Password Requirements: Many websites that require the user to create an account also have rules on how the password should be structured and what types of characters need to be present. This question aims to assess what type of password the different cloud storage providers require the users to use.

Password Change Reminder: To keep user account safe users needs to regularly change their passwords. This question aims to asses if the providers provide some type of reminder for the user to change their password after an amount of time has passed.

Two-Factor Authentication: Two-Factor Authentication as become an important way of securing accounts by requiring an extra authentication step. This question aims to assess if the cloud providers provide two-factor authentication to its user and to what degree it is pushed. For example, does the user need to use it or is it just an extra security feature that the user can choose to use?

Authentication Alternatives: There are many different ways to authenticate that are not a password. This question aims to assess the other authentication alternatives the different cloud storage providers offer their users.

Remote log out of account on old devices: Users can log in on the same account on many different devices at the same time. When a user switches a device or upgrades to another device it can be hard to remember to log out of the account from the old device. This question aims to assess if the providers provide a feature where users can see what devices their accounts are logged in to and if they are able to log out from those devices.

Extra Security Features: Many cloud storage service providers can offer several extra security features that can differ from provider to provider. This question aims to assess what other security features the cloud providers offer to their users to protect their accounts.

5 Results

This chapter will present the results from both the survey and the comparative analysis that has been conducted. Both the survey and the comparative analysis are the result of the literature review we have done to write the theoretical background. The respondent's answers from the conducted survey regarding password management, account management, and overall threat handling in a cloud storage environment will be presented here. The result of the conducted comparative analysis of the four cloud storage providers (Google Drive, Dropbox, Apple iCloud Drive, and Microsoft OneDrive) will also be presented here.

5.1 Cloud Storage security practices Survey

The survey was opened for respondents to answer on the 4th of April 2023 and was closed on the 18th of April 2023. The survey was open for a total of 15 days and the survey received 40 unique respondents. The survey was aimed at individuals that have used or are using storage as a service. The goal of the survey was to get an overview of users' general usage, practices, and security the users implement while using a storage-as-a-service solution. The full survey can be found in Appendix A.

Figure 5.1 visualizes how the participants have chosen their cloud storage service based on preset alternatives. 67% of the 40 respondents answered that they choose their cloud storage service based on convenience over anything else. Previous experience and pre-installed on the device saw an equal distribution of 15% or 6 respondents each. Only one respondent answered that they choose their cloud storage service based on its security features.

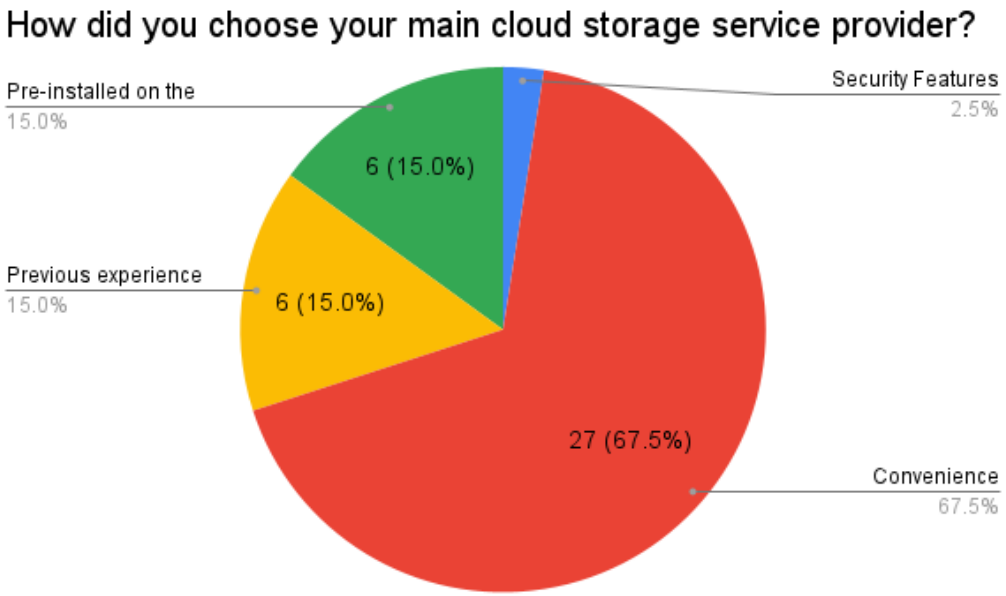

Figure 5.1: Distribution of respondents practice when choosing a cloud storage service

When the respondents were asked the question “Do you know of your account details being leaked, if so what measures did you take afterward?” 23 or 57,7% of the respondents responded that they did not know of their account details being leaked. If the respondent was aware of their account details being leaked, 7 respondents responded that they changed their password and 10 respondents responded that they not only changed their password but also implemented additional security features. None of the 40 respondents answered that they did nothing despite knowing that their account information had been leaked, see Figure 5.2.

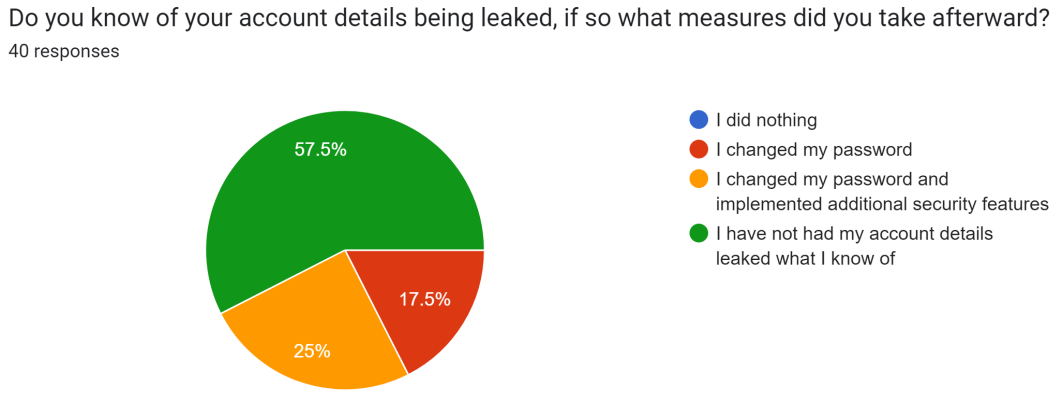

Figure 5.2: Distribution of respondents’ answers to the question "Do you know of your account details being leaked, if so what measures did you take afterward?"

Of the 40 respondents, 67,5% answered that they log out of their cloud storage accounts from devices that will be replaced, restricting account access from the old devices. 32,5% of the respondents answered that they do not log out of their cloud storage accounts, see Figure 5.3 for a visual representation of responses.

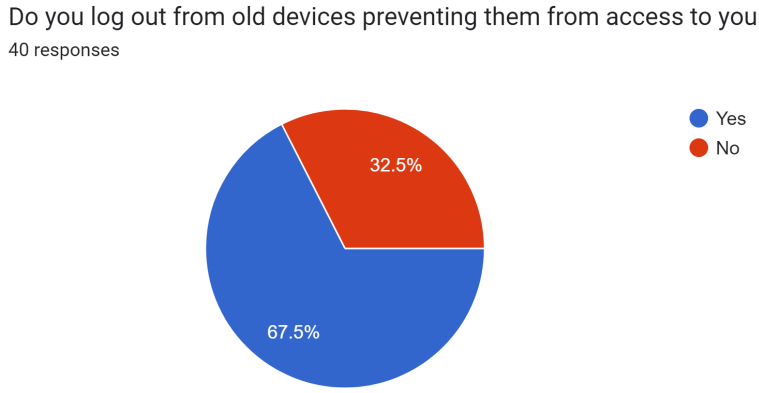

Figure 5.3: Distrubution of respondents that log out their account from old devices

Among the respondents, 21 or 52,5% answered that they implement some additional security feature to their cloud storage account. 12 or 30% of the respondents stated that they do not implement any security features and just implement the minimum security to get the service to work. On the other hand, 7 or 17,5% of the respondents stated that they implement all security features that are provided by the service provider, see Figure 5.4 for a visual representation of the respondent's answer distribution.

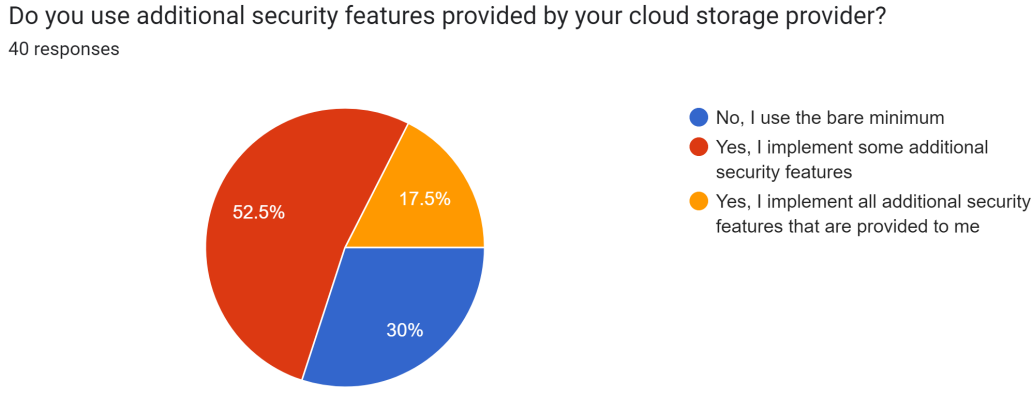

Figure 5.4: Distrubution of respondents' answer regarding implementing security features

When the respondent was asked about what password security practices fitted them the best regarding their password management. The answer “I don’t use known bad passwords” got a total of 27 responses while the answer “I don’t reuse old passwords” got 21 responses. When it comes to password storage 20 respondents stated that they use a password manager to keep track of their passwords. 17 respondents stated that they check to see if their password has been in a data leak. Only 9 out of the 40 respondents said they regularly change their password. 4 respondents stated that they did not implement any practices to secure their passwords, see Figure 5.5.

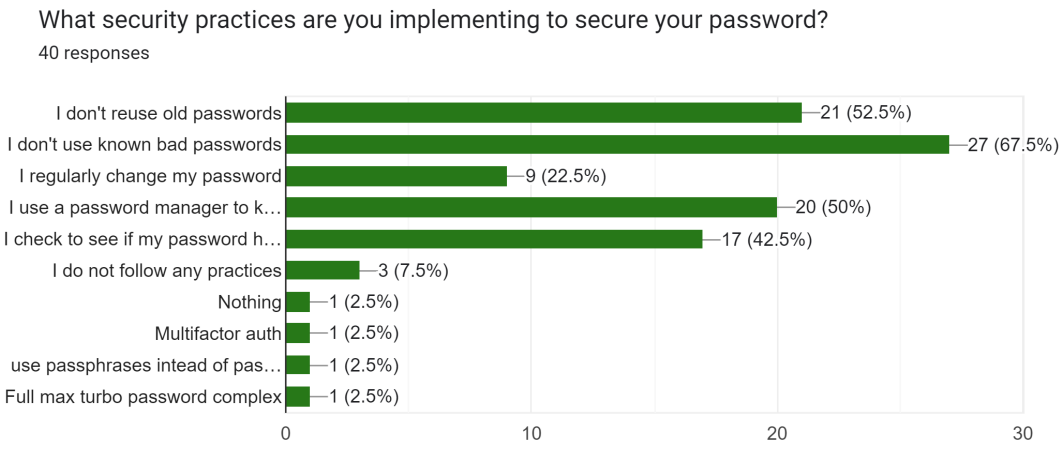

Figure 5.5: Respondents distribution of the multichoice question "What security practices are you implementing to secure your password? "

Among the respondents, 14 or 35% stated that they created their own password/passphrase following a security standard, and 9 or 22,5% of the respondents answered that they created their own password without following a security standard. The majority of the respondents, 16 or 40% answered that they use an autogenerated password and are not creating their own. One respondent stated that he uses a random object ID when creating the password, see Figure 5.6.

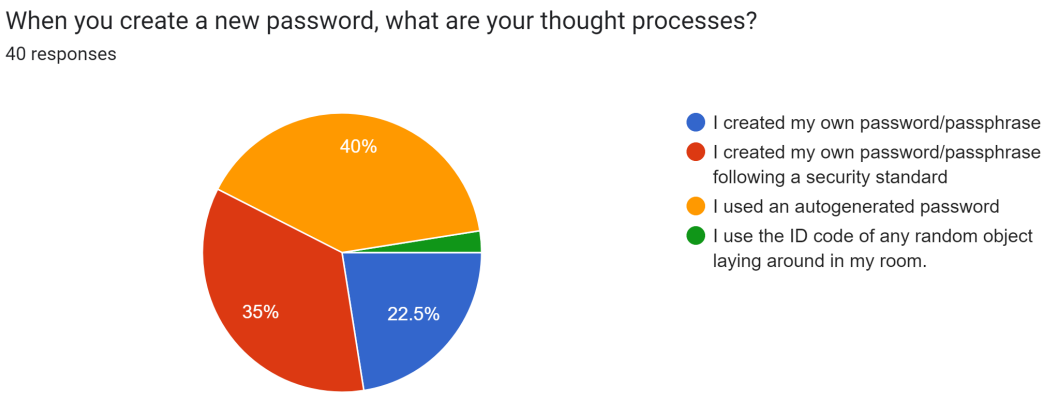

Figure 5.6: Respondents distribution of thought process on password creation

The respondents were asked from which networks they access their cloud storage. 19 or 47,5% of the respondents answered that they access their cloud storage from any network that they are connected to. Out of those 19 respondents, 11 or 57,8% respondents stated that they are aware of the risks in accessing their cloud storage from any network, but are still doing it. 14 or 35% of the respondents answers that they access their cloud storage from networks they trust are safe and 7 or 17,5% of the respondents stated that they access their cloud storage only from networks they know are safe, see Figure 5.7.

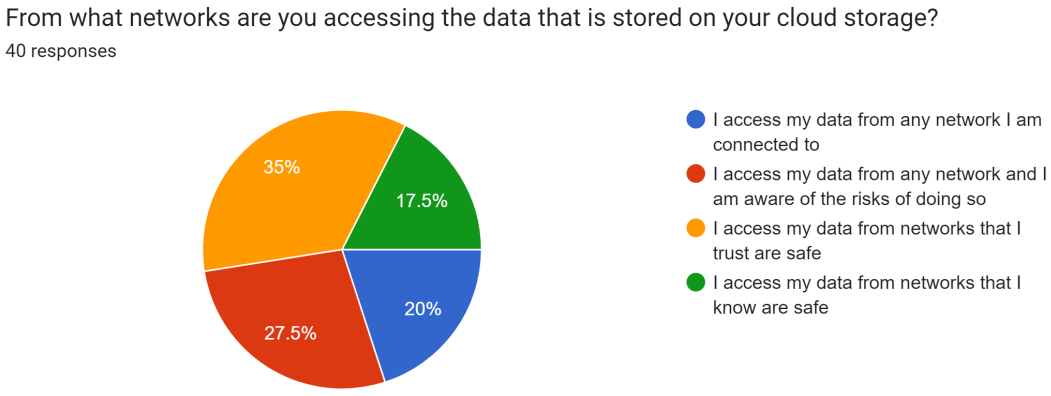

Figure 5.7: Respondents' distribution of from which network they access their cloud storage service

The respondents were asked what they would do in a situation where they receive an email stating that they need to change their password. The majority of the respondents 30 or 75% stated that they would check the email's validity and determine if it is true or false before acting on any information in the email. Nine respondents or 22,5% stated

that they would follow the instructions but would not click on any provided links in the email. They would instead go there by their own intuition. One respondent stated that they would follow the email instructions and press provided links without determining the email validity first, see Figure 5.8.

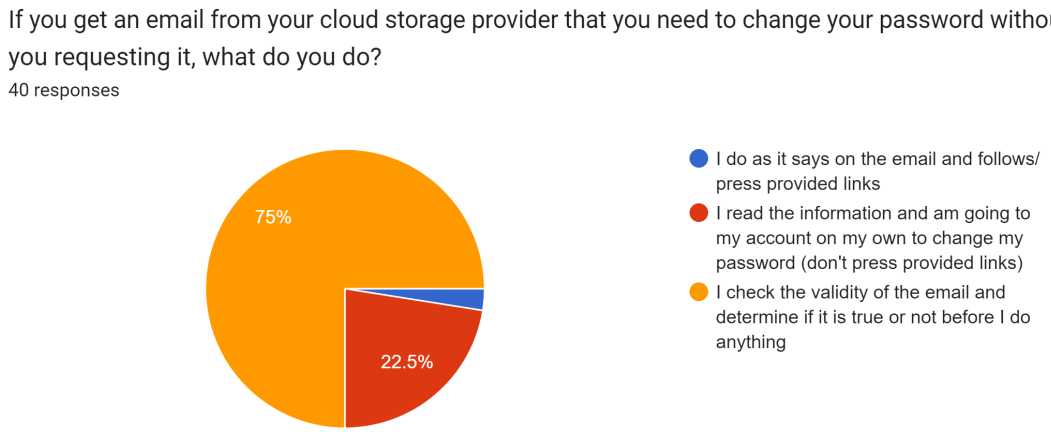

Figure 5.8: Respondents' distribution of email security practices

5.2 Comparative Analysis

In this comparative analysis we aim to answer RQ3, our main focus is to examine the security features provided to users by popular Cloud Storage service providers. The survey shows around half of the participants do not implement additional security features, seeing what security options can be implemented can increase this number. Furthermore, we check if the features can mitigate the Security threats from RQ1. We will also closely evaluate the password requirements of these providers. We will carefully examine these providers' password requirements as well. For this investigation, Google Drive, Dropbox, Apple iCloud Drive, and Microsoft OneDrive were the chosen Cloud Storage service providers. The providers were picked based on the standing of their brands as well as the availability of a trial edition.

5.2.1 Google Drive

When creating a new Google account the minimum requirement of a password is at least eight characters and a combination of letters, numbers, and symbols. Compared to other services, Google does not have a prompt to inform the user if their inputted password is weak or strong. Google offers login using mobile, two-factor authentication, or Security keys as a security option. The user must independently search for and activate these options. It also has features for recovery phones and recovery emails.

Additionally, Google has a list of devices which is connected to the account. This list allows the user to locate the device, remotely sign out from the devices, and see device information. Google also gives tips on what to do if something seems not right when managing the devices.

5.2.2 Dropbox

When creating a new DropBox account the minimum requirement of a password is 6 characters but it does not enforce what type of characters are mandatory in the password. For example, a password as "aaaaaa" is allowed but it is considered weak by a prompt besides the password creation. according to this prompt, a strong password would at least be 11 characters long and does not have a repetition of characters throughout the password, such as "abc abc". Through the security settings, it is possible to see all devices connected to the account. It is possible to remotely disconnect a device from the account, which means the device will stop synchronizing and have no access to the account's files until it is reconnected. This is a great feature if a device is no longer used by the owner or if it has been stolen. But If the account is authenticated through a Google account and the device is logged in as well on that Google account, then it only requires pressing one button to get access again to the account, no password is needed. Which is a security threat.

DropBox has two-step verification implemented but as default, it is turned off. The user, therefore, needs to activate this service if they want to use it. To activate the two-step verification the user must input the account's password, and choose between using SMS or using one of the phone application that DropBox support for two-step verification. These apps can be Google Authenticator for Android/iPhone, Duo Mobile for Android/iPhone, and Authenticator for Windows Phone 7. The application needs to scan a QR code. When the user inputs the code it will give the user 10 one times backup codes and the two-step verification is activated.

DropBox also provides security control for the user, which is a five-step process: Verification of email address, Review of connected devices and browsers, Review of connected apps, Improve password, and check two-factor authentication settings. Users who have received a notification of login from an unknown device are directed to this check. Dropbox also has a feature where the user's password expires as a security measure and must therefore be periodically updated. There is no indication of how often a password must be updated.

5.2.3 Apple iCloud Drive

When setting up a new Apple ID, the password must be at least eight characters long, including one uppercase letter, one lowercase letter, and a number. Apple also advises against using a password that is associated with other accounts. During password creation,

users receive feedback on the strength of their password. To achieve a strong password rating, a password must be at least 16 characters long, but repetition is allowed. For example, a password consisting of "aB1" repeated until the 16-character threshold is met will be considered strong.

Account registration also requires a valid phone number for two-step authentication, which is mandatory for all new accounts and cannot be disabled. Users must complete the two-step authentication process before gaining access to their accounts.

Furthermore, Apple offers app-specific passwords for non-Apple applications to enhance iCloud account security. This feature ensures that if another account is compromised, the iCloud account remains protected.

5.2.4 Microsoft OneDrive

When creating a new Microsft OneDrive account the password needs to be a minimum of eight characters long and include at least two characters each of the following types of characters: lowercase letters, uppercase letters, numbers, and symbols. There is an option available to receive a reminder for changing the password after a 72-day period. Users can also add an alternative email address for recovery purposes in case they forget their password or their account gets stolen. While Microsoft provides passwordless accounts and two-factor authentication options, users need to explore and enable them on their own.

Table 5.1: Summary of the most common security features that the cloud storage service providers offer.

Cloud Storage Servoce Provider	Google Drive	Dropbox	Apple iCloud Drive	Microsoft OneDrive
General password requirement	• At least eight charachters • Compination of letters, numbers and symbols	• At least six charachters	• At least eight characters • One uppercase letter • One lowercase letter • One number	• At least eight characters • Two uppercase letter • Two lowercase letter • Two number • Two Symbols
Two-step verification	Recomended	Recomended	Forced	Recomended
Reminder of password change	None	None	None	After 72 days
Device manager	Yes	Yes	Yes	Yes
Other authentication methods	• Security Keys • Backup 2-step verification phone • Authenticator • Backup Codes	• Security Key	• Security Key	• Security Key • Microsfot Authenticator • Code sent to Email • Biometrics or pin code • Code sent as an SMS
Other security Features	• Password Manager • Account Recovery Options • Security Questions • Find Lost device (Android) • Enhanced Safe Browsing	• Password Manager • Security Check • Backup Recovery Phone	• Password manager • Account recovery options • Find Lost device (Apple) • Option to log out from all devices when changing password • Emedently sign out from all connected browsers	• Account recovery options • Account activity monitoring

6 Analysis

This chapter will present an analysis of the result gathered from both the survey and the comparative analysis.

6.1 Cloud Storage security practices Survey

The respondents were asked about their thought process on how they chose their main cloud storage service provider. 27 respondents or 67,5% stated that they had chosen their storage service based on convenience over anything else. It can be argued that the alternatives "Previous experience" and "Pre-installed on the device" which got 6 or 15% of the answers each are a form of convenience. Only one of the 40 respondents stated that they picked their cloud storage service based on its security features. This shows that an overwhelming majority of the respondents choose convenience over security when it comes to which provider they choose.

Among the respondents, more than 65% stated that they log out of their cloud storage accounts from old devices preventing the device from accessing the cloud storage. This shows an understanding of the potential threats in keeping accounts logged in on devices that are no longer used. Among the cloud storage providers we tested, all of them have a device manager where users can remotely log out of their account from any device they have logged in to. This could be a feature that can be more pushed to the user, like a reminder if the user has not logged in to the account from a specific device after a set amount of time they would receive a notification reminding them to log out from the account if the device is no longer used.

When it comes to password management and security, half of the respondents stated that they do not reuse old passwords, a little more than half of the respondents stated that they do not use known bad passwords, and a great majority don't change their passwords regularly. This means that there is still quite a bit of people that still choose convenience over safety regarding their password practices. It is easier to reuse passwords because you don't need to remember different passwords for different services and if you combine this with a weak password it can become a great disaster. The biggest downside is that the hacker now only needs to crack one password to get access to multiple services that the user has.

60% of the respondents stated that they create their own passwords and out of those 60%, 35% stated that they follow a security standard while creating the password, which shows a greater understanding and importance of a good password. One interesting factor is that 40% of all respondents stated that they use an auto-generated password. For example, google presents autogenerated passwords when a user creates a new account on various sites. Google also prompts the user that it can save the password and user name, so the user doesn't need to remember them. This is a great convenience for many people and

provides additional password security. But it comes with two major disadvantages, the user must now rely on Google to keep their password safe, and if a hacker compromises the account the hacker now has access to all the services that Google have saved username and passwords. To further increase security users can download and use a trusted third-party password manager to keep their passwords safe and 50% of the respondents stated that they are currently using a password manager.

The respondents were asked if their account details to their cloud storage service had been leaked at some point and what countermeasures they took afterward. 23 out of the 40 respondents or 57,5% stated that their account details have not been leaked what they aware of. The answer can be interpreted in two ways, either the respondents are not aware of how to look up if their account details have been leaked and are unaware, or the respondents know how to identify if their account details have been leaked and know that it has not been leaked. The remaining respondents stated that they had identified that their account details had been leaked and none of the 40 respondents stated that they did not do anything afterward to protect their account. 7 out of the 40 respondents stated that they changed their passwords and 10 respondents stated that they changed their passwords and implemented some extra security feature that their cloud storage provider provide. The result shows that out of those whose account details have been leaked, all of them at least changed their passwords indicating some threat and security awareness among the respondents.

The respondents were also asked if they implement extra security features or if they only implement the mandatory/bare minimum security features to get the cloud storage service to work. The majority of respondents 52,5% or 21 respondents stated that they implement some additional security features offered and 17,5% or 7 respondents stated that they implemented all security features offered to them by their provider. This shows an understanding and willingness by the respondents to increase the security of the offered service by their own intuitions. 30% of the respondents or 12 respondents said that they only implemented the bare minimum security in order to be able to use the offered service, which can show a more convenient mindset rather than a security understanding. Important to note that minimum security can differ from provider to provider, and someone that implements minimum security from one provider can in comparison have implemented more security than someone else that implemented minimum security from another provider.

When the respondents were asked what they would do in a situation where they reserve an email from a source that looks like their cloud storage service provider, stating that they need to change their password without the user requesting it. 30 respondents or 75% stated that they would check the validity of the email and first of all determine if the email is legitimate or not before following any instructions. This action shows a good understanding of security awareness and practices on how to handle potential threats sent by

email mostly known as phishing attacks. 9 respondents or 22,5% stated that they would read the information in the email but would not press any of the provided like within. Instead, the user would navigate by their own intuition to the service provider's website where the user can change the password. This action also shows understanding and awareness regarding potential threats targeting users of the service. It can be dangerous to press provided links from an untrusted source, due to the fact the links can lead anywhere where the user's authentication credentials can be stolen. Only one of the 40 respondents answered that they would follow the instructions in the email and press provided links without first determining the trustworthiness of the email. This shows a lack of understanding when it comes to email security and security practices. Interestingly, 39 out of the 40 respondents stated they would take some type of security measure when handling a suspicious email.

The respondents were asked from what networks they are accessing the cloud storage service, this was done to see if the respondents intentionally avoided accessing their cloud storage on potentially insecure networks. The result showed that 47,5% or 19 respondents stated that they access their cloud storage from any network. Out of those 19, 11 respondents stated that they do it and are aware of the potential risks in doing so, showing awareness of the risks but neglecting them. The other 8 respondents do not show awareness of the risks associated with trusting potentially dangerous and malicious networks and thereby being targeted by man-in-the-mobile attacks. Most of the respondents 35% or 14 respondents stated that they access their cloud storage service from networks that the respondent trust is safe, while 17,5% or seven respondents stated that they access their cloud storage from networks they know are safe. This shows some understanding of potential security risks and examples of mitigation strategies in only accessing their cloud storage from a more secure network minimizing the risk of being exposed to man-in-the-middle attacks.

6.2 Comparative analysis of Storage as a service

Some significant differences between these cloud storage services are brought out by comparing the security features provided by Google Drive, Dropbox, Apple iCloud Drive, and Microsoft OneDrive. One of these differences is the password requirement where Dropbox has the weakest requirements with at least 6 characters and a strong password is identified with 11 characters with only lowercase. This would take less than 3 hours to brute force compared to iCloud which will take over a trillion years, with 16 characters with numbers, symbols, lowercase and uppercase letters being identified as a strong password. Additionally, it is worth noting that only Dropbox and Apple iCloud Drive provide a password strength prompt, which can help users create stronger passwords and reduce the risk of weak passwords being used. Google Drive and Microsoft OneDrive lack this feature.

The Device management tools that these Cloud Storage Service Providers offer are a key distinction between them. All have the option to see the information on the devices connected to the account, additionally, be an option to disconnect the device remotely. However, Google Drive and iCloud Drive have the option to find the devices as well, but this only works if the device has an internet connection. These advanced features for locating lost or stolen devices, which can be helpful in maintaining the security of the account. Why they have these features can be because Google and Apple are the creator of operative systems Android and IOS. Meaning they have the right to implement such a feature into their services. Additionally, Google has a lot of tips on what to do when entering the security settings, such as if the phone is gone or if a security incident has happened.

These services all provide various authentication methods, such as two-step authentication. It's important to note, though, that only Apple iCloud Drive mandates two-step authentication, which can increase account security. The absence of two-step authentication may improve the user experience while lowering account security. The use of a security key is another authentication option that these services offer. This key enables password-free sign-in, but it requires a PIN code and a physical key to access the account. This feature can prevent hackers from accessing the account from other devices, thereby enhancing account security. Users of Microsoft OneDrive can choose to receive a code via email or SMS on a device of their choosing as a method of authentication. Users can log in without entering a password thanks to this added security measure. Users can enter the code they received instead of entering a password, making this an easy and secure authentication method. The security of OneDrive's biometric authentication has been questioned due to the overlap in different users' properties, which makes it possible for unauthorized users to access the account.

The other security features provided by the Storage as a Service provider must be manually turned on by the user for them to work, such as personalized password manager which all except OneDrive have. A password manager allows the user to save all the passwords they use behind one authentication process. which allows users to create more secure passwords without needing to remember them. This in turn can increase the password strength and security of other services at the same time while increasing quality of life. All the analyzed providers have a backup recovery option but handle it differently. The most intriguing recovery feature on Google Drive allows you to add another device for recovery. If you use two-step authentication and the primary device is missing, this is especially beneficial.

7 Discussion

When it comes to the survey answers, it is important to keep in mind that the survey got most of its respondents from the Linnaeus University general Slack channel within computer science which cover both students and teachers. This means that most of the respondents may have a greater understanding and usage of computer systems than the average cloud storage user may have. This can therefore give a slight bias towards a greater security mindset than if the survey had reached a broader audience. It is therefore important to have this in mind while analyzing the survey answers and drawing conclusions about user security practices.

When analyzing the answers from the survey some questions had a different outcome than what was expected and some followed the predicted outcome. When analyzing how the respondents choose their main cloud storage service provider, it was identified that the was majority chosen their cloud storage based on convenience and only one choose based on the security feature. This was an expected outcome where the majority are comfortable with what they already know. It can be hard to convince some to switch just because another provider has better security features and it is therefore important that the provider implements and informs its users about the security features that it offers. One survey question answer that had an unexpected outcome was that 40% or 16 respondents stated that they use autogenerated passwords. It was expected that the majority would create their own in some way. The outcome of the unexpected distribution can most likely be explained as follows, many popular browsers like Google Firefox and Safari can autogenerate passwords for its user when they tried to create an account using the web browser. The username and password can then be saved in the browser and automatically filled in when the user later tries to authenticate for the service. This has given auto-generated passwords an increase in convenience because now the users do not need to remember the often hard and complicated auto-generated passwords. It has thereby become easier to autogenerate passwords and let the browser keep track of them, rather than coming up with a password that fits all the requirements yourself. This would explain why we see the majority of the respondents use autogenerated passwords.

Another thing to keep in mind is that some of the survey questions might give a false impression at first glance. For example the question “Do you use additional security features provided by your cloud storage provider?” where one of the answers is “No, I use the bare minimum” might hint that the respondent doesn’t use that much security for their account, but that might not be true depending on which provider is used. Different cloud storage service providers have different minimum security requirements for their services. For example, Apple iCloud Drive requires users to add a phone number when creating an account, thereby adding two-factor authentication by default, while other cloud storage providers may have other minimum requirements where two-factor authentication is not required. The question still shows that those who actively seek extra security features may

have more interest in securing their accounts actively, while those who don't are satisfied with what security they get by setting up the account or are unaware of extra security features due to a lack of advertisement for them.

During the research, it became clear that differences in security features among the chosen Storage as a Service providers. They have many similarities as well as many differences. These differences can have a large impact on user account security and may influence the user's security choices.

Firstly, password requirements and strength guidelines vary across cloud storage services. Dropbox has the weakest requirements, making user accounts potentially more vulnerable to brute-force attacks. In contrast, iCloud's strong password requirements significantly enhance account security. Password strength prompts, as seen in Dropbox and Apple iCloud Drive, can encourage users to create more secure passwords, whereas the lack of this feature in Google Drive and Microsoft OneDrive might result in weaker passwords being used. However, providing a password strength prompt should not be an excuse for allowing users to create weak passwords.

Device management tools also differ among the cloud storage services. Google Drive and iCloud Drive offer advanced features such as remote disconnection and device location options, enhancing account security. These features are more prominent in these services due to their close ties with Android and iOS operating systems. On the other hand, Microsoft OneDrive and Dropbox offer more basic device management options. This management option is more than enough for cloud services.

Two-step authentication plays a crucial role in account security. While all the services provide this option, only Apple iCloud Drive mandates its use, striking a balance between user experience and security. Non-mandatory two-step authentication might result in a better user experience but can lower account security.

Alternative authentication methods, such as security keys and receiving codes via email or SMS, offer advantages and disadvantages. Microsoft OneDrive's biometric authentication, for example, raises security concerns due to overlapping user properties. This could potentially lead to unauthorized account access. Alternatives such as receiving codes via email and SMS can be a secure and password-free experience, but action for the user to take out a phone or get access to an email account can lead to a lower user experience when logging in. Using security key authentication could be the most secure method, as it requires not only access to a specific device but also the presence of a physical security key with a pin code during the login process. All services offer this as an alternative, likely due to its recognition as a highly secure option.

8 Conclusions

In conclusion, the research that has been done has succeeded in identifying threats that are targeting users of cloud storage services. The conclusion drawn from the identified threats is that the threats are mostly targeting the user account and user authentication credentials and it is therefore important that users have proper knowledge of account management security. Many of the identified threats are not only limited to cloud storage services but can also impact other types of services that require users to have an account to be able to use the service. Both users and providers need to work together to increase the security of the service, providers need to implement security features and advertise them and the user then needs to implement and use those security features. It is a team play where users and providers need to work together to increase the overall security of the service.

The conducted survey was successful in gathering information regarding user security practices in a cloud storage environment. The result from the survey shows that a majority of the respondents show a good understanding and practice while utilizing a cloud storage service. The survey shows some tendencies that respondents rather choose convenience over security in some situations but that the respondents overall have quite a high-security understanding. This can be misrepresented and does not reflect how a "normal user" may be thinking and acting in the same situation. Because the survey got most of its answers from students and teachers who all have an orientation toward computer science, and they might therefore have a higher security awareness than if the majority of the respondents would have been business majors or nursing students.

After analyzing the security features of four popular cloud storage services, it is clear that each platform has different strengths and weaknesses. But there are several similar features, as everyone is allowing two-step authentication but to different degrees, device management that allows disconnecting devices remotely, and an alternative option of authentication. Google Drive has strong options for device management and recovery but lacks prompts for strong passwords and defaults to the user finding and enabling two-factor authentication. Dropbox's password requirement is weaker than the others. Apple iCloud Drive has strict password requirements and mandatory two-step authentication. Microsoft OneDrive has several authentication options for password-less accounts.

Overall, users should carefully consider the security features and requirements of each cloud storage service and take additional measures, such as regularly updating passwords and enabling two-factor authentication, to further protect their data.

8.1 Future Work

The result of this thesis work lays the ground for future research in the area of cloud storage security and practices among users. Because cloud services are such a wide area of study, there is a lot of potential future work that can deepen the field of study. For

example, future work could expand the survey to include more detailed questions and spread the survey in a different way to get more generalizable answers. Another approach could be to focus on one specific threat and go into more detail about the specific threat or to focus on different demographics and see if there is a difference in security practices between them. When gathering data one must not only do a survey, one could try to conduct interviews instead and compare the two data sets for a better understanding and to verify the result.

References

[1] IBM.com. Data storage defined. [Accessed: 8 Mar 2023]. [Online]. Available: https://www.ibm.com/topics/data-storage

[2] R. Sheldon. (2022, Oct) direct-attached storage (DAS). [Accessed: 8 Mar 2023]. [Online]. Available: https://www.techtarget.com/searchstorage/definition/direct-attached-storage

[3] IBM Cloud Education. (2022, Mar. 14) Storage area network (SAN) vs. network attached storage (NAS). [Accessed: 8 Mar 2023]. [Online]. Available: https://www.ibm.com/cloud/blog/san-vs-nas

[4] aws.amazon.com. What is cloud storage? [Accessed: 8 Mar 2023]. [Online]. Available: https://aws.amazon.com/what-is/cloud-storage/

[5] cloud.google.com. What is cloud storage? [Accessed: 8 Mar 2023]. [Online]. Available: https://cloud.google.com/learn/what-is-cloud-storage

[6] S. I. Bairagi and A. O. Bang, "Cloud computing: History, architecture, security issues," in *National Conference "CONVERGENCE*, vol. 2015, 2015, p. 28.

[7] ibm.com. What is cloud computing? [Accessed: 15 Mar 2023]. [Online]. Available: https://www.ibm.com/topics/cloud-computing

[8] P. M. Mell, "The nist definition of cloud computing," National Institute of Standards and Technology (NIST), Special Publication 800-145, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[9] intel.com. Storage as a service: Defining your public cloud storage strategy. [Accessed: 15 Mar 2023]. [Online]. Available: https://www.intel.com/content/www/us/en/cloud-computing/storage-as-a-service.html

[10] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: a brief review," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 421–426, 2019.

[11] checkpoint.com. The biggest cloud security challenges in 2021. [Accessed: 15 Mar 2023]. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-native-security/the-biggest-cloud-security-challenges-in-2021/

[12] M. Jangjou and M. Sohrabi, "A comprehensive survey on security challenges in different network layers in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, no. 6, pp. 3587–3608, 2022. [Online]. Available: https://doi.org/10.1007/s11831-022-09708-9

[13] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57 792–57 807, 2021.

[14] A. Syed, K. Purushotham, and G. Shidaganti, "Cloud storage security risks, practices and measures: A review," Nov 2020. [Online]. Available: https://www.researchgate.net/publication/348167335_Cloud_Storage_Security_Risks_Practices_and_Measures_A_Review

[15] O. Andersson, "En värdering av molntjänsters risker och förebyggande åtgärder," 2022.

[16] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The journal of supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020.

[17] A. E. Widjaja, J. V. Chen, B. M. Sukoco, and Q.-A. Ha, "Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study," *Computers in Human Behavior*, vol. 91, pp. 167–185, Feb 2019.

[18] ImmuniWeb, "Top 10 cloud security incidents in 2022," https://www.immuniweb.com/blog/top-10-cloud-security-incidents-in-2022.html, 2022, accessed: April 14, 2023.

[19] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of business research*, vol. 104, pp. 333–339, 2019.

[20] J. Linaker, S. M. Sulaman, M. Höst, and R. M. de Mello, "Guidelines for conducting surveys in software engineering v. 1.1," *Lund University*, vol. 50, 2015.

[21] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf *et al.*, "Nist cloud computing reference architecture," *NIST special publication*, vol. 500, no. 2011, pp. 1–28, 2011.

[22] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *Journal of Reliable Intelligent Environments*, vol. 7, pp. 69–84, 2021.

[23] H. B. Patel and N. Kansara, "Cloud computing deployment models: A comparative study," *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, 2021.

[24] S. El Kafhali, I. El Mir, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, no. 1, pp. 223–246, 2022.

[25] S. A. Sheik and A. P. Muniyandi, "Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review," *Cyber Security and Applications*, vol. 1, p. 100002, 2023.

[26] Intel, "Storage as a service: Defining your public cloud storage strategy," https://www.intel.com/content/www/us/en/cloud-computing/storage-as-a-service.html, accessed: April 13, 2023.

[27] HPE, "What is storage as a service?" Web page, accessed: April 12, 2023. [Online]. Available: https://www.hpe.com/us/en/what-is/storage-as-a-service.html

[28] A. S. Gillis, "What is storage as a service (staas) and what is it used for?" Storage. TechTarget, 2019, accessed: April 13, 2023. [Online]. Available: https://www.techtarget.com/searchstorage/definition/Storage-as-a-Service-SaaS

[29] L. F. A. Roman and P. R. Gondim, "Cloud-based authentication and key management protocol for advanced metering infrastructure in smart grid," *Transactions on emerging telecommunications technologies*, vol. 33, no. 12, 2022.

[30] D. B. Salvakkam and R. Pamula, "Messb–lwe: multi-extractable somewhere statistically binding and learning with error-based integrity and authentication for cloud storage," *The Journal of supercomputing*, vol. 78, no. 14, pp. 16 364–16 393, 2022.

[31] X. Wang, "Research on computer network security policy of cloud computing," *Journal of physics. Conference series*, vol. 1533, no. 3, pp. 32 044–, 2020.

[32] checkpoint.com. Top 15 cloud security issues, threats and concerns. [Accessed: 11 Apr 2023]. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

[33] polymerhq.io. (2022, Jun. 28) What is cloud account hijacking? [Accessed: 11 Apr 2023]. [Online]. Available: https://www.polymerhq.io/blog/insider-threat/what-is-cloud-account-hijacking/

[34] fortinet.com. What is a brute force attack? [Accessed: 12 Apr 2023]. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack

[35] imperva.com. Brute force attack. [Accessed: 12 Apr 2023]. [Online]. Available: https://www.imperva.com/learn/application-security/brute-force-attack/

[36] K. T. Hanna. (2021, Sep) brute-force attack. [Accessed: 12 Apr 2023]. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/brute-force-cracking

[37] M. S. NADEEM. (2022, Jun. 10) Top 5 bad password habits. [Accessed: 12 Apr 2023]. [Online]. Available: https://blog.mailfence.com/bad-password-habits/

[38] L. Grigas. (2022, Apr. 1) Learning password security jargon: Dictionary attack. [Accessed: 12 Apr 2023]. [Online]. Available: https://nordpass.com/blog/what-is-a-dictionary-attack/

[39] imperva.com. Phishing attacks. [Accessed: 7 Apr 2023]. [Online]. Available: https://www.imperva.com/learn/application-security/phishing-attack-scam/

[40] cloudflare.com. What is a phishing attack? [Accessed: 7 Apr 2023]. [Online]. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/

[41] cisco.com. What is phishing? [Accessed: 7 Apr 2023]. [Online]. Available: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

[42] NortonLifeLock employee. What are browser hijackers? [Accessed: 13 Apr 2023]. [Online]. Available: https://nordpass.com/blog/what-is-a-dictionary-attack/

[43] A. S. Gillis. (2021, Sep) browser hijacker (browser hijacking). [Accessed: 13 Apr 2023]. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/browser-hijacker

[44] K. Yasar. (2022, Apr) man-in-the-middle attack (MitM). [Accessed: 6 Apr 2023]. [Online]. Available: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

[45] imperva.com. Man in the middle (MITM) attack. [Accessed: 6 Apr 2023]. [Online]. Available: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[46] cloudflare.com. What is a denial-of-service (dos) attack? [Accessed: 11 Apr 2023]. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[47] K. Ferguson. denial-of-service attack. [Accessed: 11 Apr 2023]. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/denial-of-service

A Appendix

Cloud Storage security practices

Hello, our names are Hugo Joo Jonsson and Vilgot Karlsson and we are studying Network Security at Linnaeus University in Växjö. We are currently working on our thesis work regarding cloud storage security with a focus on user security. We would appreciate your participation in this survey regarding users' security practices while using a cloud storage service. If you are using or have used a cloud storage service like Google Drive, Dropbox, Apple iCloud Drive, or Microsoft OneDriveas part of your private life, we would appreciate it if you took a few minutes to answer our questions. The answers are confidential and will be used only for this research project, the survey will take a maximum of 5 minutes to complete thanks in advance.

How did you choose your main cloud storage service provider? (Required)

- Security features ( )
- Convenience ( )
- Previous experience ( )
- Pre-installed on the device ( )
- Other: ( )

Do you know of your account details being leaked, if so what measures did you take afterward? (Required)

- I did nothing ( )
- I changed my password ( )
- I changed my password and implemented additional security features ( )
- I have not had my account details leaked what I know of ( )
- Other: ( )

Do you log out from old devices preventing them from access to your cloud storage? (Required)

- Yes ( )
- No ( )

Do you use additional security features provided by your cloud storage provider? (Required)

- No, I use the bare minimum ( )
- Yes, I implement some additional security features ( )
- Yes, I implement all additional security features that are provided to me ( )

What security practices are you implementing to secure your password? (Required)

I don't reuse old passwords [ ]
I don't use known bad passwords [ ]
I regularly change my password [ ]
I use a password manager to keep track of my passwords [ ]
I check to see if my password has been in a data leak [ ]
I do not follow any practices [ ]
Other: [ ]

When you create a new password, what are your thought processes? (Required)

I created my own password/passphrase ( )
I created my own password/passphrase following a security standard ( )
I used an autogenerated password ( )
Other: ( )

From what networks are you accessing the data that is stored on your cloud storage? (Required)

I access my data from any network I am connected to ( )
I access my data from any network and I am aware of the risks of doing so ( )
I access my data from networks that I trust are safe ( )
I access my data from networks that I know are safe ( )

If you get an email from your cloud storage provider that you need to change your password without you requesting it, what do you do? (Required)

I do as it says on the email and follows/press provided links ( )
I read the information and am going to my account on my own to change my password (don't press provided links) ( )
I check the validity of the email and determine if it is true or not before I do anything ( )
Other: ( )