FEDERAL UNIVERSITY OF THE STATE OF RIO DE JANEIRO

CENTER OF EXACT SCIENCES AND TECHNOLOGY

SCHOOL OF APPLIED INFORMATICS

Data Security in Cloud Computing

CAROLINA DE CARVALHO MARCHIORO

Supervisor

MORGANNA CARMEM DINIZ

RIO DE JANEIRO, RJ – BRAZIL

DECEMBER OF 2019

Catalogação informatizada pelo autor

M315

Marchioro, Carolina de Carvalho
Data Security in Cloud Computing / Carolina de Carvalho Marchioro. -- Rio de Janeiro, 2019.
64 p.

Orientadora: Morganna Carmem Diniz.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Estado do Rio de Janeiro, Graduação em Sistemas de Informação, 2019.

1. Segurança na Nuvem. 2. Nuvem. 3. Ataque. I. Diniz, Morganna Carmem, orient. II. Título.

Data Security in Cloud Computing

Carolina de Carvalho Marchioro

Undergraduate thesis and graduation project presented at the School of Applied Informatics at the Federal University of the State of Rio de Janeiro (UNIRIO) in order to obtain the title of Bachelor in Information Systems.

Approved by:

_____

Prof. Dra. Morganna Carmem Diniz (UNIRIO)

_____

Prof. Dr. Sidney Cunha de Lucena (UNIRIO)

_____

Prof. Leonardo Luiz Alencastro de Rocha (UNIRIO)

RIO DE JANEIRO, RJ – BRAZIL.

DECEMBER OF 2019

Acknowledgments

To my mother, my first and greatest teacher. Thank you for giving me the tools and opportunities to make my way in life. For teaching me to always question the world around me, and showing me that we can accomplish anything we set our minds to. You are fiercely loyal and deeply caring, and I am so glad to call you friend as well as mother.

To my father, who never once complained about getting out of bed at 11pm to pick me up so I would get home safe. Your strength and love are endless, and you showed me that hard work and honesty always pay off. I hope to always be someone you are proud to call your daughter.

To my sister, who has shown me more patience than I've ever deserved. You gave me a second home and kindness during the loneliest times in my life. You've never been critical or made me feel like a failure, even when I've deserved it. I hope to one day have the strength to take on the world as you do, with empathy, generosity and humor.

And finally, to my grandfather Fransisco. You were one of my favorite people in the world, and some of my fondest memories are of us on your farm. I miss you. I wish you could have seen me grow up. I hope you would love the woman I've become as much as you loved the little girl who was obsessed with horses.

RESUMO

A computação em nuvem como modelo para serviços de software tornou-se uma solução cada vez mais popular para empresas e indivíduos. O enorme crescimento e adoção de soluções de computação em nuvem traz muitos benefícios, mas também riscos, principalmente em relação à segurança. A computação em nuvem tornou-se notória ao longo dos anos por suas violações de segurança, sejam elas fotografias de celebridades ou informações particulares sobre dados do usuário e padrões de comportamento. A segurança dos dados, em particular, tornou-se um tópico importante em torno da computação em nuvem devido à natureza crítica de qualquer possível violação. Recentemente, preocupações com privacidade de dados foram além da consternação popular e entraram em legislação, com muitos países propondo leis sobre privacidade e criptografia de dados. Diante desse cenário contemporâneo, esta pesquisa investiga e analisa o estado atual da segurança da computação em nuvem, principalmente no que diz respeito à segurança dos dados. Nossa análise é dividida em três categorias distintas: uma visão geral da arquitetura de computação em nuvem e problemas gerais de segurança, os padrões de segurança implementados por três softwares de segurança de dados em nuvem corporativos diferentes e uma análise dos diferentes ataques que podem ser realizados contra o referido software, as vulnerabilidades que eles procuram explorar e suas contramedidas.

Palavras-chave: Nuvem, Segurança na Nuvem, Ataque.

ABSTRACT

Cloud computing as a model for software services has become an ever more popular solution for both businesses and individuals alike. The enormous growth and adoption of cloud computing solutions brings many benefits, but also risks, especially in regard to security. Cloud computing has become notorious over the years for its security breaches, be they celebrity photographs or private information about user data and behavioral patterns. Data security, in particular, has become a hot topic surrounding cloud computing due to the critical nature of any potential breach; data privacy concerns recently have gone beyond popular consternation and into legislation, with many countries proposing laws regarding data privacy and encryption. Given this contemporary scenario this research investigates and analyzes the current state of cloud computing security, particularly in regard to data security. Our analysis is broken up into three distinct categories: an overview of cloud computing architecture and general security problems, the security standards implemented by three different enterprise cloud data security softwares, and an analysis of the different attacks which might be carried out against said software, the vulnerabilities they seek to exploit and their countermeasures.

Keywords: Cloud, Cloud Security, Attack.

Index

Figure Index

Table Index

1- Introduction

1.1 Motivation

Cloud computing as a model for software development, storage and communication has become a staple of twenty-first century technology. Almost everyone uses it in their day-to-day life, even if unknowingly. It has made many services such as file sharing, data storage and resource management easier, cheaper and more accessible. These are all welcome changes until the issue of security is analysed. Because while cloud computing may be a practical and widespread approach, it's security standards leave much to be desired. Data leaks, security breaches and ransomware threats have become notoriously tied to cloud computing software models, and as this technology continues to grow there is an ever-increasing need for better and more reliable security standards and solutions.

It's not for nothing that cloud services, particularly data storage, have become so popular in recent years. Traditional approaches to data storage, such as in-house servers, present a series of drawbacks that are easily addressed by data storage in the cloud such as the need to install and maintain physical hardware and infrastructure on premises, as opposed to the scalability of a remote Cloud server. The scalability of cloud servers means that any kind of data expansion should be reasonably accommodated by the cloud service provider, which makes data expansion a non-issue so long as the costs of expanding the cloud resources are properly accounted and budgeted for. The availability of cloud services is another big factor in considering cloud data storage. Storing data or running applications on the cloud means that employees can connect and access needed information anytime from anywhere, without the added complexities of VPNs. Data stored on cloud servers can be backed up anytime, diminishing the losses in the event of a disaster scenario. Most cloud providers also offer uptime guarantees, so while outages do occur every once in a while, they are usually short and trivial compared to the

potential downtime of an in-house server. When in-house servers suffer an outage for whatever reason, recovery of data or systems or the wait time for replacement equipment and diagnosis and repairs can be very lengthy.

Cloud data storage clearly comes with a series of benefits for most organizations looking to improve their access to data. However, cloud data storage does come with a series of cons as well, chiefly among these data privacy and security. Even though large cloud service providers invest substantial resources into implementing and researching state-of-the-art security solutions for their cloud services, as we will observe in this research there are some kinds of cloud-specific attacks which they might still fall prey to, resulting in the loss or tampering of customer's data. Also, storing critical data on the cloud may be an issue as often times third-party applications will have access to cloud data.

For a prime example we might look at our own school, the School of Applied Informatics at the Federal University of the State of Rio de Janeiro. The current solution of in-house data storage servers often presents challenges such as long periods of downtime, infrastructure maintenance, difficulties in employees accessing necessary information, not to mention the substantial and ever-increasing quantities of important data which need to be carefully backed up as the loss of student and teacher records could impede the entire school from functioning. Migration of data storage to the cloud could be an interesting solution that might address many of the current issues. However, the confidential and delicate nature of much of this data, mainly students and teachers personal information, records and projects, means that security and privacy concerns surrounding the storage of the school's data is not inconsequential and are the reason why many organizations may still hesitate to migrate their data services to a cloud environment. Data privacy is also becoming a law in many countries. Storing data in the cloud can result in sensitive data that is stored in places where laws are stricter than those in the data source territory. For example, the Brazilian General Data Protection Act (LGPD) and the EU General Data Protection Regulation (GDPR) require stricter

protection for personal data of individuals within countries under their jurisdiction. These requirements also apply to companies located in other regions of the world.[1]

Because of this, in this research we will be taking a closer look at security standards and vulnerabilities present in cloud computing, particularly data storage services.

1.2 Objectives

This paper consists of an exploratory research through an international literature review regarding state-of-the-art cloud computing security. The objective of this research will be to compile and analyze recent tendencies in cloud computing security solutions by addressing critical attacks and countermeasures that have been brought to light in recent years. In order to do that, we seek to address some of the security concerns surrounding cloud computing software, especially data security, by making an in-depth analysis of current cloud computing security standards, vulnerabilities, and solutions. We will contrast these to current deployed cloud computing data storage softwares and compare their implemented security standards to those being proposed in recent literature. We will then analyze some of the most critical attacks that can be carried out against cloud software, their origins, means and countermeasures.

1.3 Organization of the text

The following monograph will be structured as follows:

Chapter II: Research background into the different kinds of Cloud Computing technologies, their main security risks and breaches as well as currently implemented or proposed security solutions according to state-of-the-art software and research literature.

[1] Available at https://leadcomm.com.br/2019/05/17/desafios-de-seguranca-na-nuvem/ access on Dec 15, 2019.

Chapter III: This chapter looks at three similar cloud computing data storage softwares. Their security standards are analyzed, compared and any possible security vulnerabilities are noted.

Chapter IV: This chapter analyzes a few of the most critical threats and attacks cloud computing software currently faces. These attacks are analyzed based on how they might be carried out, which vulnerabilities they seek to exploit and also what are the possible countermeasures that might be employed against them. We will contrast these vulnerabilities and countermeasures to the cloud data storage softwares analyzed in chapter 3.

Chapter V: Here we will analyze the results of our study on cloud software security standards as well as propose future research which may be necessary within this subject matter.

2 - Research Background

In this chapter we will look at the different models of Cloud Computing and how security risks and vulnerabilities vary between them. We will address some of the main Cloud Computing security concerns and their proposed solutions. We will also talk about existing research that has been done on different cloud computing security software.

2.1 What is Cloud Computing?

The term "Cloud Computing" has circulated in the industry for over a decade and is frequently referenced as a popular solution to many storage, hardware, software, data and processing issues. But what exactly is Cloud Computing? What problems does it seek to solve? What are its limitations? At times, the purpose of this architecture can be as nebulous as the name implies. In this section we will map out the basic structure of a Cloud Computing service and architecture.

In the widest of terms, Cloud Computing could be defined as the provision of computational services (software development platforms, servers, storage, etc) over the internet and to end users. The providers of these services are referred to as cloud-computing vendors. Cloud-computing vendors are typically responsible for the back-end and hardware of the application they are selling. End users can then pay for the resources they consume to use from the cloud-computing vendor's hardware, such as memory, processing time and bandwidth.

The services provided by a cloud-computing vendor are traditionally divided into three distinct categories (Hashizume et al, 2013):

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Different cloud-computing vendors can provide some or all of these different types of services, depending on their requirements and business model. Let's breakdown the characteristics and differences between these categories of services:

- Software as a Service

  SaaS or Software as a Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network (Internet).

  Traditionally, software applications needed to be purchased upfront and then installed on to a computer. SaaS users, on the other hand, utilize software online and periodic subscriptions are the most common payment method, as opposed to one-time payments. A majority of SaaS applications are run directly through the web browser, and do not require any installation on the client side.

  Common tasks performed using SaaS are accounting, invoices, email, document storage, etc.

- Platform as a Service (PaaS)

  PaaS or Platform as a Service provides varied environments to allow developers to build applications and services. Developers essentially rent everything they need to build their application, relying on the cloud provider for development tools, infrastructure and operating systems.

  The main offerings included by PaaS vendors are development tools, middleware, operating systems, database management and infrastructure.

- Infrastructure as a Service (IaaS)

  Infrastructure as a Service (IaaS) also known as Hardware as a Service (HaaS) delivers cloud computing infrastructure, including servers, network, operating systems, and storage through virtualization technology. These cloud servers are typically provided to the end user though a dashboard or an API, giving IaaS clients complete control over the entire infrastructure. IaaS provides the same capabilities and technologies as traditional data center, but there is no need for the end user to physically maintain it. They can access their servers and storage directly through the cloud.

The relationship and dependencies between these layers can be represented through Figure 1, where each layer may affect the other above or below.

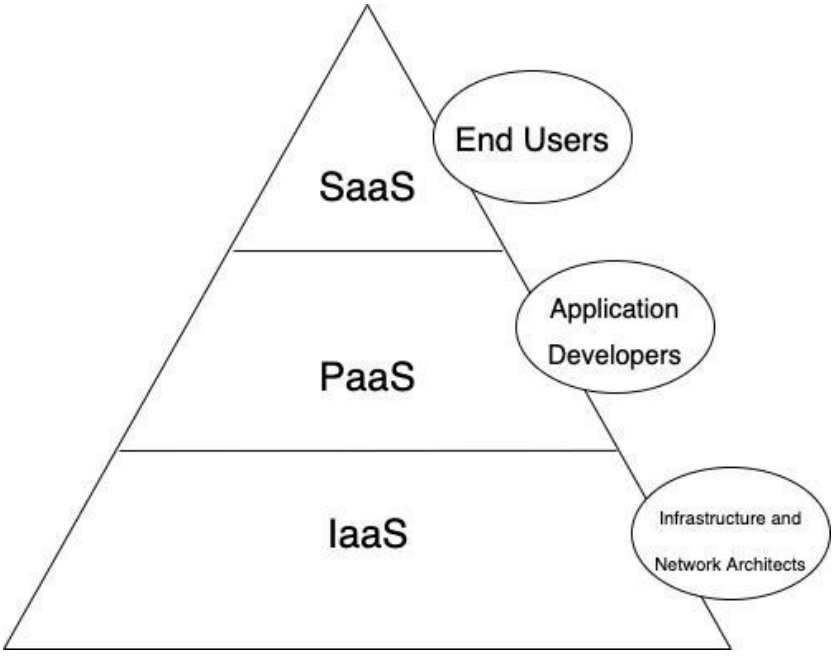

Figure 1: Different layers of cloud service models

2.2 Security Challenges Throughout the Different Cloud Service Models

We have successfully defined the different types of Cloud Computing services, their target users, objectives and products. Now we will look at the challenges present

throughout these different models, in particular those pertaining to Security. What are the most current and pressing of these security challenges? What are some of their currently proposed solutions? Over the years Cloud Computing solutions have become notorious for their security breaches, and in this section we will discuss and analyze the root causes and challenges behind some of these security vulnerabilities and threats.

With SaaS the burden of security lies with the cloud provider, due to the high degree of abstraction and integrated functionality which means the end customers have very little control. Conversely, PaaS offers some control to the end user, and IaaS more than either of the previous models (Hashizume et al, 2013).

Because of the dependencies between these three models, namely the fact that PaaS and SaaS are hosted on top of IaaS, any security breach in IaaS will necessarily impact the other two. The same goes for PaaS security breaches affecting SaaS. Any attack to a cloud service layer can compromise the upper layers (Hashizume et al, 2013). Below we will analyze some of the main security threats regarding these three models.

- SaaS

  Since application in SaaS are typically delivered through a web browser, security challenges in SaaS can be very similar to those in any web application technology. However, when it comes to SaaS, traditional solutions can only go so far. There are a variety of security threats unique to SaaS and Cloud Computing as a whole that need to be dealt with as well (Subashini and Kavitha, 2011).

  Patel *et al* (Patel and Rekha, 2014) divide the different kinds of security threats as follows into eight distinct categories: Authentication and Authorization, Data Confidentiality, Availability, Information Security, Data Access, Network Security, Data Breaches, Identity Management and Sign-on Process.

- Authentication and Authorization: the lack of access to physical hardware may generate the need for new authentication and authorization processes.
- Data Confidentiality: data privacy is an especially sensitive issue in our current society and breaches of private information are a big risk, be they intentional or not. Special care has to be taken with any entity's data that is being stored online.
- Availability: resources and data should be readily available to the appropriate personnel.
- Information Security: strong encryption techniques are one example of a measure to safeguard against malicious attackers and other security breaches that may result in stolen data.
- Data Access: while end users are ultimately responsible for data access and deciding which users get access to what information, SaaS must be flexible and robust enough to adhere to the permission policies put forward by their end users.
- Network Security: the voluminous data that flows through the networks connecting SaaS solutions to their end users must be secure.
- Data Breaches: since data from so many different companies and individuals is all stored together, a single data breach into one of these entities may compromise all of them. This makes any breach much more serious as it stops being an isolated event.
- Identity Management and Sign-on Process: ID management is a big challenge in information security which becomes even more crucial and complicated when applied to an SaaS provider.

- PaaS

  Devi and Genensan (Devi and Ganesan, 2015) define the main categories of PaaS security vulnerabilities as Interoperability, Host Vulnerability, Object Vulnerability, and Access Control. They can be defined as follows:

  - Interoperability: this feature is what allows code to be written using more than one cloud provider, and on more than one level (SaaS, PaaS or IaaS).
  - Host Vulnerability: since in cloud computing a breach in a host's security also compromises the tenants and users, special care has to be taken.
  - Object Vulnerability: since service providers can access and modify a user's object, Devi and Genensan have listed three ways in which this might cause a security breach:
    - A provider may access a user object maliciously. This kind of attack is very expensive to prevent, and is usually only avoidable when there is trust between a provider and users.
    - Users may attack each other's objects if they are tenants of a same host. This is because tenant objects share the same resources.
    - Third party attack. This is usually solvable with secure encrypting.

- IaaS

  Chawki et al (Chawki et al, 2018) list two interesting areas of security vulnerability in IaaS models. These are SLA (Cloud service-level agreement) security issues and networking security issues. Additionally, Morsey et al (Morsey et al, 2010) lists three additional areas of IaaS

security issues which are VM Security, Virtual Network Security and Hypervisor Security. While these might be older they are still very much relevant to contemporary cloud computing security:

- SLA security issues: An SLA is an agreement between a cloud service provider and a customer that ensues a minimum level of service will be maintained. While SLAs are very much necessary and important to depict the availability and user's data privacy, there exists no standardization to perform an SLA between two parties. This means that CSPs might attempt to hide or leave out many necessary parameters in an SLA that would safeguard users data and privacy.
- Networking security issues: Due to the complexity of cloud architecture networks they are vulnerable to a series of attacks, as we will see in later chapters.
- VM Security: VM's must be secured both against traditional security threats such as malware and viruses, and also against cloud-specific threats such as malicious code injection into offline VM images. Traditional security is usually the responsibility of the consumer, while VM images are the responsibility of the cloud provider. Cloud providers are also responsible for securing the boundaries of their VMs.
- Virtual Network Security: since various tenants share the same network infrastructure this increases the vulnerability of DNS servers, DHCP and IP protocol vulnerabilities.
- Hypervisor Security: "A hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice-versa" (Morsy et al, 2010). This means that a hypervisor is the main controller of any access to the physical server resources by VMs. Therefore, any security violation of the hypervisor also puts the VMs at risk.

2.3 Security Solutions

Since Cloud Computing is a relatively new and ever-changing technology, the solutions to security issues are a hot research topic, with dozens of frameworks and services coming forward to present their solution as the new market standard. Below we will discuss some of the solutions to the problems identified above proposed by past research.

- Identity and access management: this can be anything from multifactor authentication to credentials and Secure Shell keys (SSH). CSA's Identity and access management guidance details different policies and solutions to implement in these regards.
- Attribute-based Proxy Re-Encryption: proposed by Jeong-Min Do *et al* (2011) as a solution to Data Confidentiality issues in Cloud Computing environments. Their proposed system models divides the data file into header and body while the scheme selectively delegates decryption rights using Type-based Proxy Re-Encryption. This is a cryptographic scheme in which a proxy is able to convert ciphertext encrypted under a public key into ciphertext that can be decrypted by a secret key. Data confidentiality would be guaranteed by dividing the data into header and body. Through this the data owner can selectively delegate decryption rights for all or part of the data.
- Data dispersion: a commonly used solution to availability issues, data dispersion permits data to be reproduced through a distributed storage infrastructure. It allows a service provider to offer storage services based on the level of the user's subscription.
- Information Security Risk Management Framework (Zhang et al, 2010): The Information Security Risk Management Framework proposed by Zhang *et al* is only one example of a framework that

can be applied by cloud providers to do risk mitigation in regard to Information Security. This framework consists of seven processes: selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Each process is necessary to clarify specific roles, responsibilities, and accountability for each major process step.

Strong encryption techniques are another common safeguard against malicious attackers and data leaks.

- Multi-user access policies (Ion et al, 2011) and Data Access Management (Basescu et al, 2011): two examples of frameworks proposed as solutions to Data Access security risks. Ion *et al* (Ion et al, 2011) shows the implementation of a scheme that allows making SQL-like queries on encrypted databases in a multi-user setting while preserving access rights. Basescu *et al* (Basescu et al, 2011) proposes a security management framework which allows providers of Cloud data management systems to define and enforce complex security policies.
- Network security for virtual machines (Wu et al, 2010) and Network Security Sandbox (Xiaopeng et al, 2010): Both are interesting solutions for Network Security issues. Wu *et al* (2010) proposes a virtual network framework aimed to control the intercommunication between virtual machines. Xiaopeng *et al* (2010) presents a framework (VNSS) which provides both a guarantee of distinct security level requirement and full lifecycle protection for a virtual machine to provide continuous protection for a virtual network environment.

The solutions and problems proposed above are but a general look at the immense scope that is cloud computing architecture and the problems it presents. In the next chapter we will narrow the scope of our research by analysing particularly data storage cloud

softwares. In the subsequent chapters we will look at the functionalities and security measures currently implemented in enterprise cloud data storage softwares, and see what kind of attacks might be carried out against them, which would be most critical in terms of data loss, and which vulnerabilities they might exploit.

3 - A Look at Security Standards in Enterprise Cloud Software

In the previous chapter we presented the most common and widely recognized Cloud Computing security issues and solutions. Clearly, there is a wide and varied range to the different kinds of security breaches that may take place when dealing with Cloud software. In this chapter we will narrow the scope of our analysis and take a look at security issues that may arise when dealing with data storage on the cloud.

For this we will look at three different file hosting services: ownCloud, FileCloud and PowerFolder. We will compare the similarities and differences between them and look at possible security vulnerabilities present in their structure that could be exploited by malicious users. We will contrast these with the security measures currently employed by these softwares.

3.1 File Hosting in the Cloud

File hosting, otherwise known as cloud data storage, allows users to store their data remotely with the cloud service provider as opposed to locally on a hard drive. This means users can then access their stored data anywhere, anytime over the internet. This allows for a great range of flexibility as users can use a multitude of different devices and locations yet still have consistent access to their data. Because of this cloud data storage has become a staple of contemporary file hosting and sharing for businesses and individuals alike. There is an estimated 2 billion users of personal cloud storage as of 2019 and this number is predicted to keep growing (STATISTA, 2016).

Such widespread use inevitably gives rise to security concerns and breaches. Indeed, cloud storage is notorious for having been at the center of leaked data scandals be it

celebrity photos or private data from large corporations. In light of this we will be focusing this Cloud Computing security analysis around three different cloud data storage services. We will look at their origins and background, analyze any existing security documentation and best practices regarding their server hosting and development and see if, based on our survey of current cloud computing security standards in the previous chapter, there are any obvious breaches which might be exploited by a malicious attacker.

3.2 ownCloud

The software ownCloud (ownCloud, 2019) was released in 2010 and is a open-source web application designed to allow users to create cloud-based file sharing and data synchronization services. It was designed using PHP and JavaScript as well as popular database management systems such as PostgreSQL and MySQL (Xu et al, 2015).

In 2016 a fork of ownCloud was launched as NextCloud. Both are open source, but given the similarities between them and the fact that there is more available documentation for ownCloud we will not be analyzing NextCloud in this research.

In 2012 ownCloud issued security advisories for every known vulnerability. Previous to that date we have not been able to find any information about security measures they might have taken. These security advisories consist of documentation regarding best practices for server owners as well as resources for reporting security flaws. Taking a closer look at both the security policies in place and the additional suggested security measures to be implemented on a user level we can see the following:

- HTTPS: ownCloud strongly encourages an encrypted HTTPS connection for the user's server, as well as routing any unencrypted traffic through HTTPS. This is to prevent a man-in-the-middle attack.
- SSL configuration: default SSL configurations are often not state-of-the-art. Therefore ownCloud recommends using the Mozilla SSL

Configuration Generator as well as the Qualy SSL Labs Tests in order to generate a suitable SSL for the user's environment as well as test if the SSL is properly set up.

- Dedicated domain: users are strongly encouraged to use a dedicated domain for their ownCloud server in order to gain the benefits of Same-Origin Policy, a critical security mechanism that restricts how a document or script loaded from one origin can interact with a resource from another origin. It helps isolate potentially malicious documents, reducing possible attack vectors.
- Two-factor authentication: an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.
- SAML Authentication: Authentication information is exchanged through digitally signed XML documents. It's a complex single sign-on (SSO) implementation that enables seamless authentication.
- Active Directory integration: Active Directory is a directory service developed by Microsoft for Windows domain networks. Integrating with Active Directory means importing users from AD into the a specific database and validating user credentials when a user connects to your website.
- File locking: a mechanism that restricts access to a computer file by allowing only one user or process to access it in a specific time.
- Intrusion detection system: ownCloud recommends Fail2ban[2] which is designed to protect against brute-force attacks and to secure a login. It does this by monitoring log files for certain patterns and taking action should suspicious patterns emerge.
- Password policy: server administrators have the option of enforcing password policy on their users. This can be anything from a minimum character count to special character requirements to user password expiration dates.
- Password hashing: ownCloud uses bcrypt, an adaptive hash function.

[2] Available at https://www.fail2ban.org/wiki/index.php/Main_Page Access on Dec 11, 2019

- Encryption at rest: ownCloud encrypts all physically stored data.
- Rate-limiting: ownCloud does not use any form of rate-limiting but provides documentation on how to implement it should a user choose to do so.
- ModSecurity: ownCloud makes use of ModSecurity[3], an open-source, cross-platform web application firewall. It enables web applications to gain visibility into HTTP(S) traffic. Some of its functionalities include:
    - Real-time application security monitoring and access control
    - HTTP traffic logging
    - Continuous passive security assessment
    - Web application hardening

ownCloud also has an extensive developer manual outlining security guidelines and best practices for their developers. These guidelines highlight some of the most common security problems and how to prevent them. Below is a condensed list of the security breaches ownCloud developers should take steps to prevent:

- SQL Injection: ownCloud recommends always using prepared queries to prevent this.
- Cross site scripting: despite the fact that ownCloud uses Content-Security-Policy to prevent the execution of inline JavaScript code developers are still required to prevent Cross-Site-Scripting (XSS)[4]. To do this, ownCloud recommends never using the PHP functions **echo, print() or <%=** but to instead use **p()** which will sanitize the input. Additionally, URLs must be validated to start with the expected protocol (e.g. http).

  HTML must not be manipulated directly via JavaScript as this can often lead to XSS due to unsanitized variables.
- Clickjacking[5]: ownCloud prevents clickjacking by including a specific header in all template responses.

[3] Available at https://modsecurity.org/ Access on Dec 11, 2019
[4] Available at https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) Access on Dec 10, 2019
[5] Available at https://www.owasp.org/index.php/Clickjacking Access on Dec 10, 2019

- Code executions and file inclusions: to prevent this in PHP user-input should never be allowed to run through the following functions:
    - include()
    - require()
    - require_once()
    - eval()
    - fopen()

- Directory traversal: Directory traversal is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files.Sanitizing the file path (removing all / and \) prevents this attack
- Shell injection: PHP code that executes commands should always escape every user parameter. If not, attackers may be able to execute arbitrary shell commands on the server.
- Authentication bypass/ Privilege escalations: ownCloud offers three simple checks using the App Framework to prevent users from performing unauthorized actions.
- Sensitive data exposure: developers should take care to always store user data or configuration files in safe locations and not in the webroot where they could be accessed by attackers.

Notable security measures currently not implemented in ownCloud which might further improve their security is Access and Monitoring Control, Mobile Device Management, Built-in Ransomware Protection and FIPS 140-2 (U.S government security standard for cryptography).

3.3 FileCloud

FileCloud (getfilecloud, 2019) originally launched in 2012 which runs on Apache web server. File Cloud is web-based file transfer solution that offers comprehensive file and

folder management, multiple permission levels, file encryption, and large file storage. It provides a way to securely store, share, or send large files (like spreadsheets, databases, multi-media documents, etc.) at any time, from anywhere.

It is not an open source project therefore public information about the development practices is limited. However, FileCloud has written some documentation for users regarding their security standards, the most notable of which are listed below:

- Encryption at rest: FileCloud uses 26-bit AES SSL encryption, an advanced encryption standard is used for data at rest (data stored physically).
- Active Directory integration: Active Directory is a directory service developed by Microsoft for Windows domain networks. Integrating with Active Directory means importing users from AD into the a specific database and validating user credentials when a user connects to your website.
- Two-factor authentication: an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.
- SAML Authentication: Authentication information is exchanged through digitally signed XML documents. It's a complex single sign-on (SSO) implementation that enables seamless authentication.
- Granular user and file sharing permissions
- Client application security policies
- Enterprise antivirus integration
- Unlimited file versioning
- File locking: a mechanism that restricts access to a computer file by allowing only one user or process to access it in a specific time.
- Endpoint device protections
- Anti-virus scanning/ Ransomware protection: FileCloud supports scanning of uploaded files using ClamAV[6], an open source antivirus

[6] Available at https://www.clamav.net/ Access on Dec 10, 2019

software.

- Remote wipe: the administrator can remotely wipe the FileCloud data off a compromised device
- Audit reporting: activity logs closely monitor user action within the system.
- HTTPS: Apache server on which FileCloud runs can be configured to secure the web application with HTTPS protocol.
- Storage level encryption and file encryption
- SSL/TLS for secure file transmission

Since FileCloud is not open source, there is no public information on their developer's coding practices to prevent security breaches. Judging from the available public information, a possible flaw in their security measures could be the lack of an intrusion detection system.

3.4 PowerFolder

Originally released in 2012, PowerFolder (Powerfolder, 2019) is a European-based file synchronization service. It is not open source, however there is an open source PowerFolder client which may be run using the free edition of PowerFolder server.
Notable PowerFolder security features include:

- Encrypted transfers between servers and clients utilizing AES/RSA encryption algorithms.
- Device authentication and verification using RSA encryption.
- SSL support for mobile apps and web.
- Client-side encryption using cryptomator[7]
    - Encrypted transfers of data.
    - Encrypted storage of data at rest.
    - Encrypted communication between clients.

[7] Available at https://cryptomator.org/ Access on: 29 Nov, 2019

- Central user management: Centralized user management allows IT the control and visibility over every device, application, or network across the organization, without dictating what resources are the right choice for each group. Central control over users ensures that digital assets stay within the organization.
- Multi tenant system
- Granular permission system: Granular permissions are used to grant system privileges, allowing you to construct site-specific roles with privileges to match your requirements, and restrict system administrators and database owners from accessing user data.
- Password protection and expire dates on file links
- Administrator remote deletion: allows an administrator to remotely delete compromised accounts or data.
- Protection against XSS (Cross Site Scripting) attacks: the documentation does not specify exactly what this protection entails or how it is developed, only that it exists.
- Protection against man in the middle attacks: the documentation does not specify exactly what this protection entails or how it is developed, only that it exists
- Integration of Antivirus solutions directly with the server.

Possible security flaws for PowerFolder include no File Locking, no Two Factor Authentication, no SAMLAuthentication and no Network Share Versioning.

These softwares offer a few different hosting options and prices as shown in the table below.

Pricing	ownCloud	FileCloud	PowerFolder
Pricing Model	-Free -Annual subscription -Quote-based	-Monthly payment -Annual subscription -Quote-based	-Free -Annual subscription
Hosting Options	Self-Hosted Cloud Hosted	Self-Hosted Cloud Hosted Multi Tenancy	Self-Hosted Cloud Hosted
Price 50 users/year	Two price ranges: USD 3,600 USD 9,000	Three price ranges: USD 2,500 USD 6,000 UDD 9,000	Two price ranges: USD 1,300 USD 5,400

Table 1: Comparison of cloud data storage software features

3.5 An attempt at security testing cloud data storage software

One of the first ideas surrounding this research was to carry out a series of penetration tests against the cloud data storage softwares above in order to test their security standards in an ethical hacking endeavor. However, we quickly ran into some core difficulties, namely that the penetration tests we were able to carry out did not test the security of the cloud servers *per se,* but of the local network on which we carried out the tests. However, below we will briefly discuss the work that was carried out as it still speaks to the necessity of establishing good network security standards, as well as showcases the cloud data storage softwares efficacy at safeguarding against amateur penetration attacks.

The first step was to build a virtual environment on which to carry out the security testing against these three softwares. This environment consisted of a local network and host computer containing the following specifications.

- Operating system: Windows 8 version 6.3 build 9600
- CPU: Intel(R) Core(™) i7-5500U CPU @2.40GHz
- RAM: 8.0 GB DDR3 @ 1600MHz
- Graphics: NVIDIA GeForce 840M Integrated RAMDAC 4020 MB
- Hard Drive: 910 GB NTFS

On the host computer three virtual machines were created. They utilize the hardware specifications of the host computer and consist of a Kali Linux-based machine for running the penetration tests, a Ubuntu-based machine for hosting the cloud servers and a Windows 7 based machine to act as the end user of the cloud servers. All three virtual machines are run on Oracle VM VirtualBox version 6.0.12. Utilizing these machines we attempted to carry out some penetration attacks which may commonly affect other users of cloud-based storage services. The specifications for these machines are as follows.

- Machine 1: Kali Linux

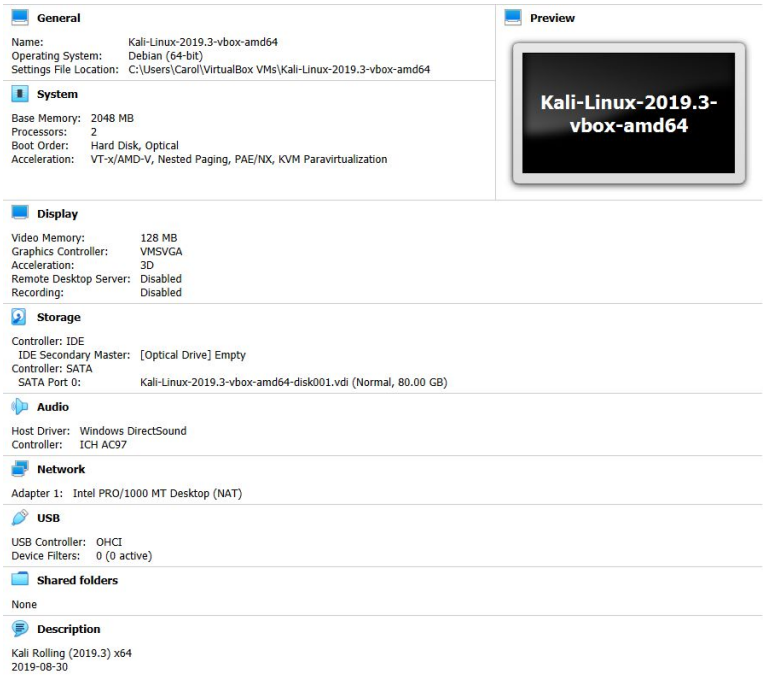

Figure 2: Kali Linux penetration testing machine

- Machine 2: Server Host

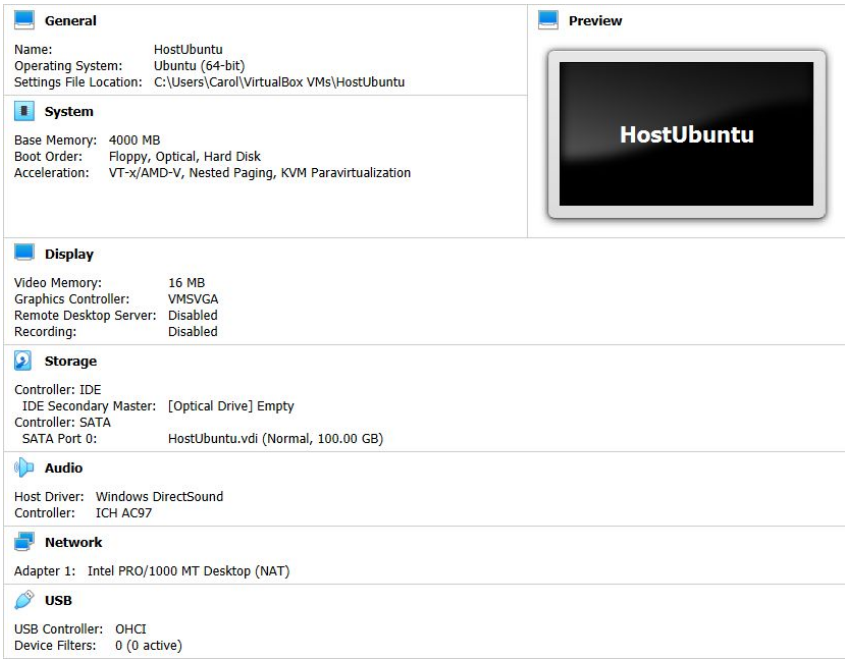

Figure 3: Cloud server host machine

- Machine 3: End User

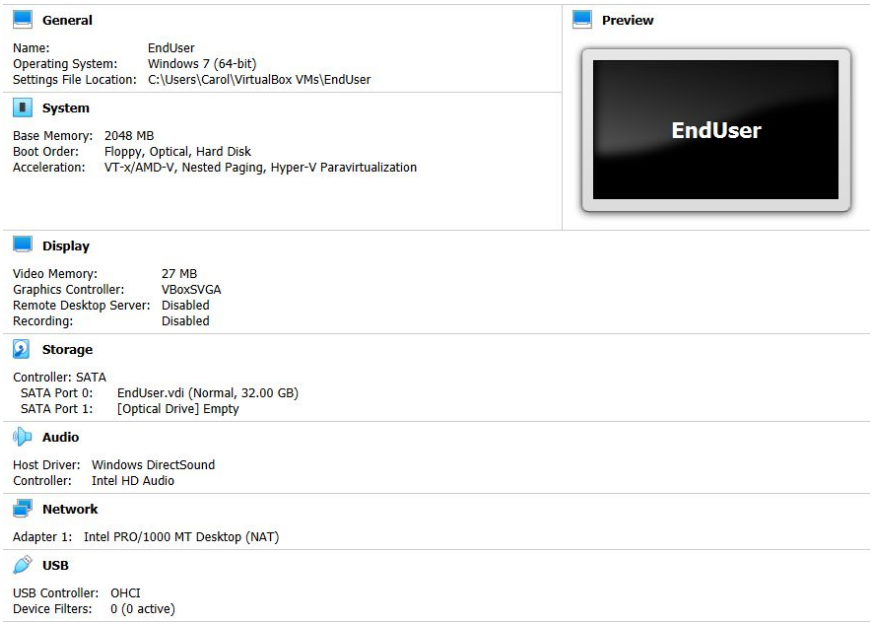

Figure 4: End user machine

After setting up this virtual environment we proceeded to install the ownCloud community server edition on our cloud server host machine. Once the server was installed, we attempted to carry out a few simple penetration tests using Kali linux on our first machine.

The first attack was a man-in-the-middle attack, in which the attacker attempts to intercept the communication between two other computers or devices. In this scenario the attacker was our Kali linux machine, while the victim was the Windows 7 machine which was uploading an image on to the ownCloud server hosted on the Ubuntu machine. While we were able to successfully sniff out the image being uploaded to ownCloud from the victim machine, it was only because we had not enabled HTTPS encryption on our ownCloud server, which is clearly stated in the ownCloud documentation as best practice for server administrators. None of the other simple tests attempted were successful, and the majority of the attacks to be analyzed in chapter 4 are of a much more critical nature which makes them unviable to carry out in an amateur environment, so this line of research was discarded in favor of an in-depth analysis of the possible attacks and their countermeasures.

We have now established the security standards and best practices for the three cloud data storage softwares being analyzed in this research. In the following chapter we will take a look at some of the most critical attacks specifically designed to breach cloud softwares such as these, we will talk about how these attacks might be ethically executed through penetration tests and subsequently how they can be safeguarded against.

4 - Cloud Computing Attacks and Countermeasures

Besides the attacks that might be carried out against most conventional software, cloud computing opens up new avenues of attack due to the dynamic and demanding nature of its environment. Because of this, over the years, many kinds of attacks targeting cloud computing infrastructure have emerged, and other more traditional attacks have taken on a new threat in light of the vulnerabilities exposed by cloud software.

In this section we will analyze the most critical attacks which could be carried out against a cloud computing software, as well as suggested countermeasures proposed by recent literature. Despite the threat these attacks present, this analysis could also be used as a guide to ethical penetration testing against enterprise cloud software in order to verify and safeguard the currently implemented security measures. Due to the complexity of the previously analysed cloud data storage softwares as well as the critical nature of the following attacks, we will not be carrying out these tests ourselves, however the analysis may be used as a blueprint for future testing endeavors should the need and occasion arise to test and safeguard similar enterprise softwares.

4.1 Man-in-the-middle attacks

A man-in-the-middle attack (MITM) happens when an attacker intercepts the communication between two parties without their knowledge. Often the attacker will impersonate one or both of the parties attempting to communicate and gain access to confidential information. This attacks exploits the real-time processing of transactions, conversations or other kinds of data exchanges. This attack is hardly new or unique to

cloud computing however certain MITM attacks might become more pervasive due to cloud computing architecture. For example, cloud computing may be more vulnerable to wrapping attacks. Wrapping attacks occur when attacks manipulate an XML document through the XML signature element wrapping. Because cloud users typically connect to services via a web browser this increases the risk for cloud computing users to fall prey to this kind of attack.

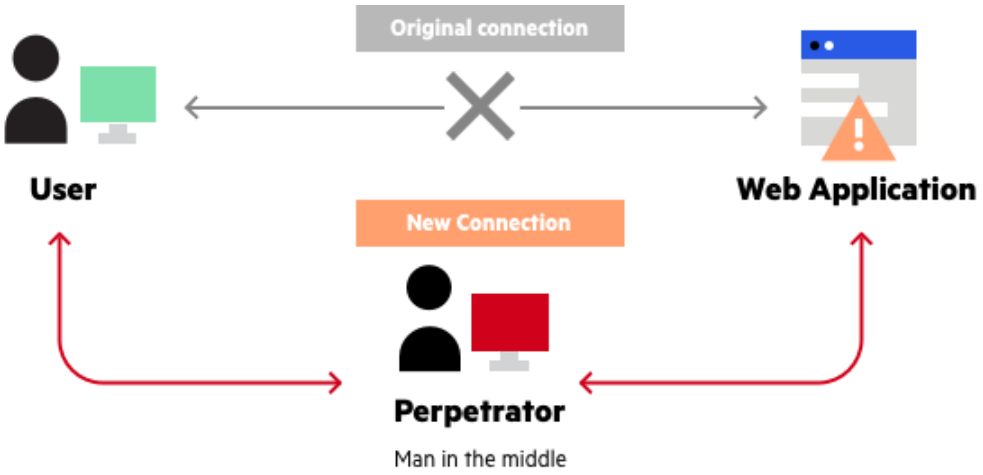

Figure 5: MITM Attack (Imperva, 2020)

An illustrative example of a man-in-the-middle attacks can be seen in Figure 5 above, in which a perpetrator attempts to intercept the communication between a web application and a user.

Solutions for this kind of attack are generally considered best practices by industry standards. They consist of utilizing proper Secure Socket Layers (SSL) architecture. SSL makes use of TCP to provide reliable end-to-end protocols (Naseer et al, 2017). Other security measures put forward by Alhenaki et al (Alhenaki et al, 2019) include the use of encryption/decryption algorithms and an Intrusion Detection System.

4.2 Man-in-the-cloud attacks

One of the most common attacks against cloud file storage and synchronization applications are the man-in-the-cloud attacks[8]. This kind of attack depends on exploiting the cloud applications synchronization protocols and end-user authentication token (Jabir *et al*, 2016). Synchronization tokens, commonly implemented in popular file share applications, save a token on the endpoint, either in the registry or in a file, after initial authentication in order to improve usability - this way users don't have to re-enter their credentials every time they wish to access their files. Man-in-the-cloud attacks exploit these synchronization token systems to gain access to cloud accounts.

Part of the danger of MITC is how difficult it can be to detect. MITC does not require any particular malicious code or exploit, and the use of well-known synchronization protocols makes it extremely difficult to distinguish malicious traffic from normal traffic (Imperva, 2015). A MITC attack might consist of a simple tool, ran through a drive-by-download exploit[9] or a simpler Phishing attack[10], which copies this authentication token from the victim's machine by modifying some specific files or registry keys and subsequently gains access to the victim's account. In some instances the attacker might even be able to maintain remote access to the victim's account for however long they choose without the victim ever becoming aware of the security breach.

The persistence of MITC attacks is part of the danger. Besides how difficult they are to detect, even if the victim does become aware of the security breach it can be extremely difficult to deny further access of the attack to the account. The attacker's synchronization token must be revoked which is not always possible depending on the synchronization application being used. Often times, the only solution should this kind of attack be successfully carried out is for the victim to cancel their current account and

[8] Available at https://www.helpnetsecurity.com/2019/01/21/mitc-attack/ Access on: 29 Nov, 2019
[9] Available at https://www.trendmicro.com/vinfo/us/security/definition/drive-by-download Access on: 29 Nov, 2019
[10] Available at www.imperva.com/learn/application-security/phishing-attack-scam/ Access on: 29 Nov 2019

open a new one, which may result in any number of inconveniences such as data loss or subscription renewals.

Given the discrete nature of this attack and how difficult it can be to detect, it is recommended preventive security measures be prioritized. These should be a mixture of software and interpersonal solutions, since this attack relies heavily on social engineering to be carried out. Best practices against MITC attacks are as follows:

- Two-Factor Authentication: Also known as Multi-Factor Authentication (MFA), this is simple but effective security measure that adds another layer of credential requirements in order for a user to log in to their account. This could be anything from a phone number or email verification to biometrics. This extra layer of security is effective at thwarting MITC attackers who are unable to authenticate beyond the synchronization token (Pressley, 2019). Unfortunately, MFA is still not as widely used as one might expect. Indeed, of the three cloud data storage softwares being studied in this research, only one (ownCloud) implements MFA as their default.

- Data Encryption: while encryption cannot prevent a successful MITC attack, it can minimize the repercussions of a successful security breach. If a MITC attacker gains access to a victim's account but all the data therein is adequately encrypted, then the data loss is significantly reduced as the attacker would not be able to access the contents of the data. This assumes the encryption key is not also stored within the cloud service. Thankfully, good encryption standards are not only expected from cloud data storage systems, they are also required by law in many countries[11]. All three of the cloud data storage softwares being studied in this research implement data encryption, both in transit and at rest. However, only ownCloud specifies the existence of a physical master key, or a master key that is not also stored in the cloud application.

- Cloud Access Security Broker (CASB): this solution was originally proposed as

[11] Available at https://www.silentcircle.com/encryption-laws/ Access on: 29 Nov, 2019

a solution to the MITC attack by Imperva[12], a reputable cyber security software company based in California. CASBs are security enforcement points between consumers and service providers that apply security controls to access cloud services, usually SaaS services (Fernandez et al, 2015). They intermediate all the traffic between an organization's cloud applications and endpoint devices, and automatically replace each application's authentication token with an encrypted variant before delivering them to the endpoints. This way, in the eventuality of a MITC attack, the attackers token would fail the validation and decryption check and deny them access to the victim's account. Of the three cloud data storage softwares analysed in this research, none seem to make use of a CASB. If they do, it is not included in the security information and documentation readily available to the general public. One theory as to why this may be is the generally significant cost of hiring a third party reputable CASB vendor which may discourage smaller companies from contracting them.

- Security training: a simple yet obvious security solution, regular employee training in best security practices and standards is very effective against a MITC attack given how heavily it relies on social engineering. A well-trained and vigilant employee is less likely to open a suspicious attachment inside a phishing email or on a malicious link. Due to the private nature of inner-organization security trainings there is no available information as to the frequency and quality or even the existence of security trainings within the three cloud data storage softwares being analyzed in this research.

Penetration testing your application for MITC vulnerabilities is another important security measure. While there is little current information about best practices for penetration tests against this attack given how recently it's emerged into the public eye, Imperva's whitepaper[13] about MITC describes different kinds of attacks which might be ethically replicated in an offensive security endeavor.

[12] Available at https://www.imperva.com/ Access on: 29 Nov, 2019
[13] Available at https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf Access on: 29 Nov, 2019

4.3 Denial-of-Service attacks

Considered one of the top cloud computing security issues of 2019[14], denial-of-service attacks, or DoS attacks, have taken on a new threat in the age of cloud computing. A DoS attack generally consists of flooding a website or other online service with more traffic than the server or network can accommodate. This is an attack on Availability, as the end goal is to render the service inoperable. While this attack can be devastating enough under the traditional software model, in the "pay-as-you-go" approach to cloud computing resource management a DoS attack may result in devastating economic loss for the victim. The very aspects of cloud computing that make it such an attractive choice for businesses, namely elasticity[15], multi-tenancy[16] and auto-scaling[17], are precisely what DoS attackers aim to exploit by causing the victims to consume an immense amount of hardware resources, which results in a very expensive service bill. This is in addition to the traditional consequences of a DoS attack which include economic loss due to downtime, reputation and brand image loss, and even data loss depending on the nature of the DoS attack (Somani et al*,* 2015).

Closely tied to DoS attacks are DDoS attacks, or distributed-denial-of-service attacks, which differ from DoS in that they launch the attack from multiple locations or computers as opposed to just one. Figure 6 below demonstrates the core difference between these two attacks,

[14] Available at https://www.cloudmanagementinsider.com/top-5-cloud-computing-security-issues-and-strategies-used-by-hackers/ Access on 30 Nov, 2019
[15] Available at https://solutionsreview.com/cloud-platforms/what-is-elasticity-and-how-does-it-affect-cloud-computing/ Access on 30 Nov, 2019
[16] Available at https://searchcloudcomputing.techtarget.com/definition/multi-tenant-cloud Access on 30 Nov, 2019
[17] Available at https://docs.rightscale.com/faq/What_is_auto-scaling.htmlAccess on 30 Nov, 2019

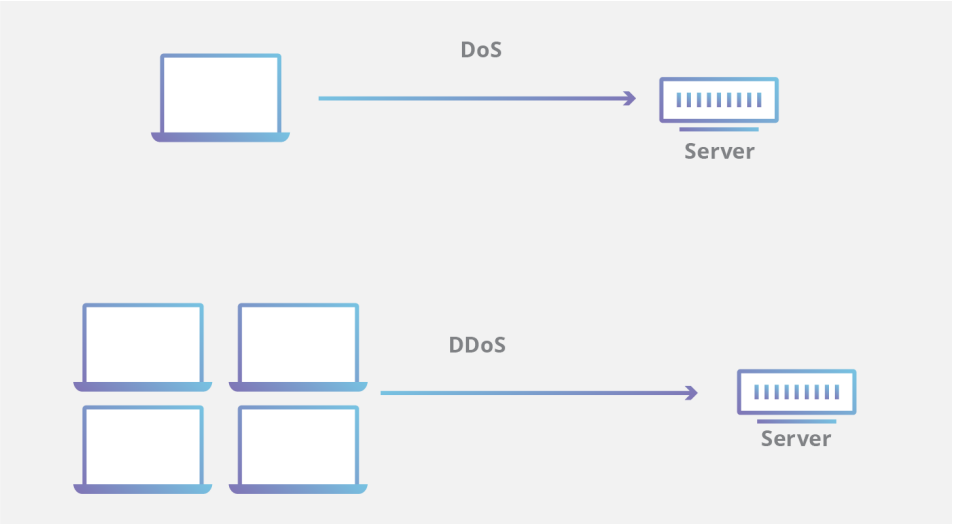

Figure 6: DoS vs DDoS (Cloudfare, 2020)

DoS attacks are typically classified into two distinct types, namely bandwidth attacks and resource depletion attacks (Bakr et al, 2019). Bakr et al define the difference between the two as follows:

> Bandwidth attacks focus on sending a large amount of traffic from single of distributed devices, the most common methods utilizing UDP protocols since UDP packet replies are much larger than their requests. On the other hand, resource depletion utilizes a wide variety of methods, sometimes it can rely on how the protocol is structured like TCP flood attacks, other times it might rely on how certain applications are written like in buffer overflow attacks. (Bakr et al, 2019, p.189)

Web application and services, especially cloud services, have become the main target of bandwidth depletion attacks. DoS solutions are still struggling to keep up with these kinds of attacks, since application-level DoS attacks can emulate the same characteristics of legitimate clients, which makes them much harder to detect and mitigate (Choi et al, 2014). Indeed, some of the most recent and relevant research being published today regarding DoS attacks on cloud software propose models and techniques to improve detection of DoS attacks.

Part of preventing and dealing with DoS and DDoS attacks comes from understanding

how they are carried out in the first place. DoS attacks can be made using a variety of tools and methods, and each one will have exploit different security vulnerabilities and have different consequences for the victim. Behal and Kumar (Behal and Kumar, 2017) propose in their paper a taxonomy of DDoS attack tools which can be categorized as per the figure below:

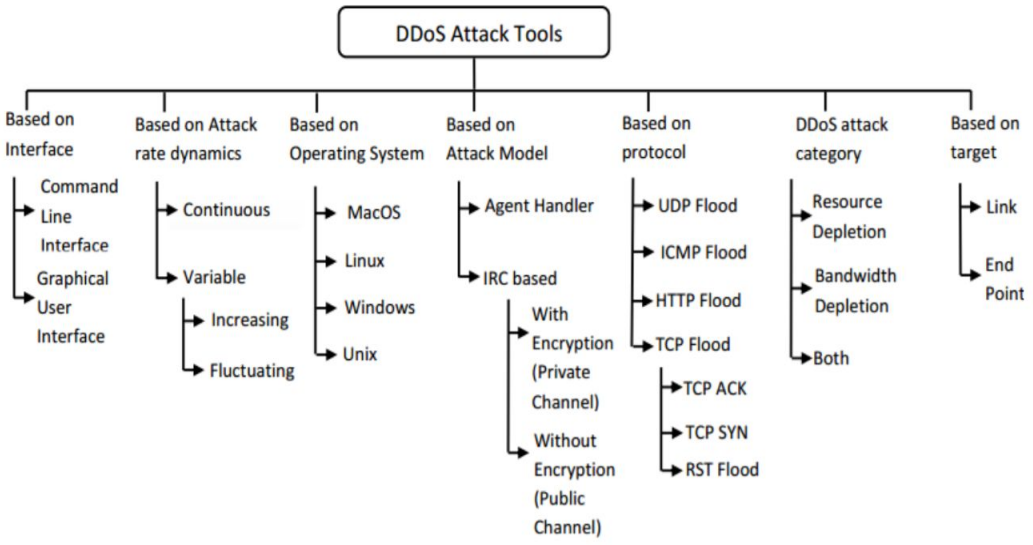

Figure 7: Taxonomy of DDoS Attack Tools (Behal and Kumar, 2017)

Figure 7 describes a series of different tools which might be utilized to carry out a variety of different DDoS attacks. Knowing which tools and methods are being used to carry out a DoS attack is critical in the eventuality of being the victim of a DoS attack. It can also be helpful for offensive security testing, in that a penetration tester might want to safeguard their system against any number of DoS attacks originating from different tools. Knowing all the avenues of attack is important when it comes to safeguarding a system.

While best practices to avoid DoS attacks is still very much an open issue, with new research frequently pointing to different solutions and techniques, Somani et al (Somani et al, 2017) present, in their research, a taxonomy for DoS attacks in cloud computing compiled from recent literature. They also discuss the challenges these techniques present and any existing issues. Here we will address some of the most relevant and

widely implemented techniques put forth in their paper.

Defense against DoS in the cloud can generally be achieved in three different ways:

- Attack prevention: this category consists of proactive techniques meant to impede as much as possible the eventuality of a DoS attack.

  Notable preventative techniques include challenge response authentication processes, in which a protocol will attempt to determine if a user is a bot/attacker machine by means of a challenge or question that the user must answer correctly in order to gain access to the system. One of the most common examples of this technique is the implementation of a Turing test in the form of a CAPTCHA (Somani et al, 2017).

  Hidden servers or ports is another frequently implemented DoS preventative measure. The objective is to remove the direct communication link between the client and server by keeping an intermediate node/proxy to work as a forwarding authority (Somani et al, 2017). Hiding resources can be used in a series of ways such as with ephemeral servers (Khor and Nakao, 2009). Hidden servers can help in preventing the malicious traffic from a DoS from affecting the real server.

  Resource limitation techniques are another important measure that might prevent the enormous economic loss that comes from a DoS attack against software hosted on the cloud. This is sometimes achieved by placing a "cap", or maximum threshold, for the resources which might be consumed from the cloud provider. However this may be a disadvantage in the eventuality of a server experiencing a surge of genuine, non-malicious traffic. A possible solution to this could be an algorithm that decides whether or not a traffic increase is malicious or genuine and allocates resources accordingly, however as we've established before differentiating between malicious and non-malicious traffic is still very much an open issue.

- Attack detection: it's nearly impossible to prevent all kinds of DoS attacks, so there should be detection and recovery controls in place for when preventative measures fail. Below are some of the most notable detection techniques proposed by recent literature:

  Anomaly detection consists of attempting to identify anomalous, or malicious, traffic usually by establishing a baseline from the behavioral patterns of regular traffic flow. Machine Learning and feature based detection solutions are often implemented for this technique. Kalai and Ranjana (Kalai and Ranjana, 2019) utilize a Hadoop framework with MapReduce to detect anomalies from a HTTP flood DoS attack. The major challenges for this technique consist in the behavior identification of the features that make up the training datasets.

  BotCloud detection is necessary when a DDoS attacker not only targets cloud services as the victim for their attacks, but also utilizes cloud infrastructure to carry out said attack. When cloud infrastructure is used for the purpose of installing botnets[18] this is known as a BotCloud. A BotCloud detection system should have a broad view of all nodes in the cloud environment, be based on cloud-core technologies and be reliable for large cloud environments while also being effective (Memarian et al, 2015). The solution proposed by Memarian *et al* consists of applying Virtual Machine Inspection (VMI)[19] and data mining techniques to separate the infected cloud VMs from the remainder. Fracois *et al* (Francois et al, 2011) propose an algorithm implemented in Hadoop to differentiate between legitimate and bot nodes.

- Attack mitigation: in the eventuality of an attack, the server should be able to continue providing access to legitimate users. Downtime is a serious issue for

[18] Available at https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html Access on 02 Dec, 2019
[19] Available at https://resources.infosecinstitute.com/virtual-machine-introspection-in-malware-analysis/#gref Access on 02 Dec, 2019

businesses which may result in economic and brand loss. Mitigation techniques aim to keep the server alive and serving requests to legitimate users even while under the effects of a DoS attack.

Resource scaling is one of the most popular features of the cloud. It is also considered to be one of the best mitigation techniques to counter DoS attacks by allowing servers to be continually available with scaled resources (Somani et al, 2017). Of course, the disadvantage of this technique is when the DoS attacker is trying to generate economic loss for the victim and so continually increases the scale of the attack until the victim is forced to either pay enormous amounts to keep their servers up and running or instead shut down and deal with the repercussions of downtime.

Software defined networking is an emerging reconfigurable networking paradigm which is changing the landscape of DoS mitigation. The separation of the data plane and control plane is the key idea behind SDN networks (Hameed and Khan, 2018). The authors propose a protocol that allows SDN controllers to safely communicate and transfer information about ongoing attacks to each other. This enables effective filtering near the source of the attack, saving time and network resources. While SDN-based is still a developing topic but one that holds great promise.

Penetration testing for DoS can be complicated due to legal issues. Depending on your cloud service provider this kind of attack may not be allowed, even in an ethical endeavor, due to the critical nature of its consequences. Even if an ethical DDoS attack is legally viable, it can still be extremely expensive due to the need to create a vast and high-quality network of bots from multiple sources. However, there are ways to test the defensive techniques of a system without creating an entire DDoS scenario, such as isolated testing of the individual components of the security measures as opposed to a full-scale penetration test.

4.4 Cloud malware injection attack

A cloud malware injection attack occurs when an attacker attempts to inject a malicious service or virtual machine into the cloud environment. The attacker will create their own malicious service implementation model (SaaS or PaaS) or virtual machine instance (IaaS) and try to add it to the cloud environment (Chouhan and Singh, 2016). The attackers objective is to have their service implementation be treated as a valid instance by the cloud system, and have traffic redirected to the malicious service in order for the malware to be executed. Should the attacker be successful, they would be able to perform any number of illegal activities such as eavesdropping, data modification, unauthorized access to cloud resources, user credential leakage, functionality changes and service blocking (Islam et al, 2016). Part of the challenge of dealing with malware injection attacks in the cloud is not only detecting it's occurrence but also determining which virtual machine instances are being used by the attacker for the malicious service implementation.

Normally a malware injection attack is done via a compromised FTP server[20]. Malware attempts to sniff FTP passwords and sends these passwords (and the user name) back to the attacker. The attacker then uses the FTP credentials to access the website in order to add malicious code to the site's web page which in turn infects other visitors who access it (Khan and Gill, 2018). In a cloud-based system, a web client's request is executed based on authentication and authorization. During this authorization and authentication process a large amount of metadata is exchanged between the web server and web browser. An attacker can take advantage of this metadata. In another form of malware injection attack, an adversary attempts to inject malicious service or code. In this case, the injected malicious service or code appears as a valid instance of services running in the cloud. If the attacker is successful, then the cloud service will be vulnerable to eavesdropping and deadlocks, the later forces a legitimate user to wait until the completion of a job, which was not generated by the user. This type of attack is also known as a meta-data spoofing attack (Khan and Gill, 2018).

[20] Available at https://www.techopedia.com/definition/26108/ftp-server Access on 03 Dec, 2019

A possible countermeasure to this kind of attack as proposed by Shaikh (Shaikh, 2016) is to perform a service instance integrity check for incoming requests. He describes this as follows:

> A hash value can be used to store on original service instance's image file and subsequently compared with the hash values of all new service instance images. As a result of using the hash values, an attacker is required to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance into the cloud system (Shaikh, 2016, p. 751)

Another proposed solution by Chouhan and Singh (Chouhan and Singh, 2016) is to use hardware for integrity purposes due to the increased difficulty in intruding at the IaaS level. A file allocation table system (FAT) might be used to determine the validity and integrity of the new instance by comparing the current and previous instances against each other. For this solution, a hypervisor should be deployed on the provider's side. This hypervisor would be responsible for scheduling all the instance and services and should check against the file allocation table to validate and integrate an instance of customer access (Chouhan and Singh, 2016).

Amongst all the malware injection attacks, SQL injection and cross-site scripting (XSS) are probably two of the most well known ones, so much so that the security standards in place to prevent them are prime examples given by the three cloud data storage softwares we've analysed previously in this research. SQL injections target SQL servers that run vulnerable database applications by injecting malicious code in order to bypass the login and gain access to confidential data. Meanwhile, cross-site scripting (XSS) deals with injecting code into the data context of HTML-based documents on the client side and gaining access to sensitive data from within the server. It allows the attacker to execute scripts from within the clients' web browser. Both should be frequently tested against in order to assure the continued safety of the cloud application.
Solutions to SQL Injection as proposed by Alhenaki et al (Alhenaki et al, 2019) include appropriate filtration to sanitize user input, avoiding the use of dynamically generated SQL in the code and using a proxy-based architecture to dynamically detect and extract user input.

4.5 Authentication attacks

Any authentication mechanisms should provide high security and support user mobility but this is even more crucial for cloud applications where end users will be accessing their applications from a variety of different locations and different devices. The need to have a trustworthy yet practical authentication mechanism poses significant requirements to the security of a user authentication mechanism. Because of this, there exists numerous attacks that can exploit loopholes in different authentication mechanisms, therefore identifying the most secure authentication mechanism with high user acceptability is a big challenge in the cloud environment. Brute force authentication attacks are still very much common against applications that use only a login and password mechanism. Therefore strong password standards should be encouraged, as well as password hashing and encryption. Different authentication mechanisms should be considered such as biometrics. Authentication tokens, while frequently used, fall prey to their own set of attacks as seen previously in Section 4.2 which details the man-in-the-cloud attacks, designed specifically to take advantage of the widespread use of authentication tokens in file share softwares.

4.6 Phishing attacks

Phishing attacks affect both cloud providers and users in the PaaS cloud model (Alhenaki et al, 2019). This kind of attacks aims to manipulate a web link and redirect the user to a fake link. Should the use click this link the attack would then be able to hijack their account and gain access to confidential data. Phishing attacks are some of the oldest in the book, so there are various systems in place that allow users to easily safeguard against them, such as using anti-spam tools and pop-up blockers.

4.7 Port Scanning attacks

Port scanning is a popular form of reconnaissance that may precede another attack. It consists of the attacker sending requests to each port, asking to connect to a network.

The scan will then make note of which ports responde and which seem vulnerable. Once the attacker has determined vulnerable ports in a network, the scan will classify ports into three categories:

- Open: The host responds, announcing it is listening and open to requests. An open port means it's a path to attack the network.
- Closed: The host responds, but notes there is no application listening. Often, hackers will come back to scan again in case it opens up.
- Filtered: The host does not respond to a request. This could mean the packet was dropped due to congestion or a firewall.

Common solutions for port scanning attacks include firewalls and TCP wrappers (which allow administrators the flexibility to permit or deny access to the servers based on IP addresses or domain names). Alhenaki et al also cite packet counts, neural networks and capturing packets as possible solutions.

4.8 Cross-virtual-machine attacks

Also known as side channel attacks, cross-VM attacks target highly sensitive data and computations, e.g., cryptographic operations. They use a hidden channel that leaks information on an operation, typically execution time or cache access patterns. A side channel attack may break cryptography by using information leaked by physical parameters, such as monitoring the electromagnetic field (EMF) radiation emitted by a computer screen to view information before it's encrypted. Other well-known side channel attacks include spying on the power consumption of an electronic device to steal an encryption key, or acoustic attacks that record the sound of a user's keystrokes to steal their password. This is shown in Figure 8 below where the side channel information might be stolen to decryption the ciphertext information.

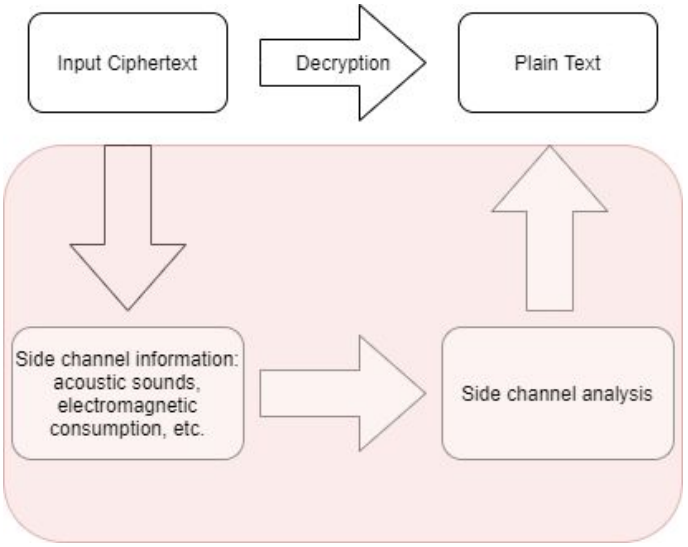

Figure 8: Side channel attack

Such "channels" are commonly created in software implementation of cryptographic algorithms. Cross-VM attacks can be applied to a wide range of computing devices from smartcards to VMs. Their impact may be greater than other attacks targeting cryptographic algorithms as they attempt to retrieve secret data without any special privileged access and in a non-exhaustive manner (Bazm et al, 2017). Proposed solutions by Alhenaki et al to this kind of attack include virtual firewalls and strong encryption and decryption protocols.

4.9 VM Rollback attacks

In this kind of attacker there is an attempt to take advantage of a VM from an old snapshot. Wani and Lone further define VM Rollback as follows:

> Virtualization is the most volatile part of cloud computing environment and to no surprise can be used to compromise virtual machines by a malicious hypervisor. The hypervisor at any point of time is authorized to suspend a VM during execution, take a snapshot of current CPU states, memory and disk and resume a snapshot afterwards without the knowledge of guest VM. This characteristic of the hypervisor is used mainly for fault tolerance and maintenance, but the attackers have exploited this characteristic of the

> hypervisor to successfully launch VM rollback attacks. The attackers take advantage of previously taken snapshots and run them without the user's knowledge. The history is cleared to avoid getting caught and the same or different snapshot can be run again (Wani and Lone, 2017, p. 101)

Alhenaki et al suggest using the suspend and resume features of VMs as defense against this kind of attack. The suspend and resume feature allows the user to save the current state of a virtual machine. When the virtual machine is resumed, the applications that were running before the suspension will resume their running state with their content unchanged.

4.10 VM Escape attack

VM escape is an exploitation by which a malware running in a VM bypasses the isolation between the host and VMs and interacts directly with the hypervisor. This provides the attacker a root privilege, access to the host OS, and possibly full control over the environment (Rakotondravony et al, 2017). This allows the attacker to read, write and execute the contents of the memory that is beyond the access of the compromised tenant (Alhenaki et al, 2019). Figure 9 below demonstrates how the attack VM might interact with the target hypervisor to access root privileges.

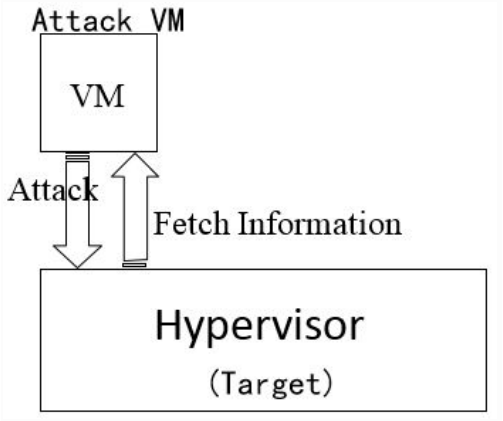

Figure 9: VM Escape Attack (Jiang et al, 2017)

Alhenaki et al recommend as security solutions to this kind of attack monitoring hypervisor activities, requiring VM isolation, using a secure hypervisor and configuring the host/guest interactions.

4.11 Countermeasures implemented in enterprise softwares

Now that we've taken a look at some of the most challenging and critical of attacks which might be carried out against cloud software we will analyse which of the proposed countermeasures are currently implemented by the previously analysed cloud data storage enterprise softwares in the table below:

Attack	Solution	ownCloud	FileCloud	PowerFolder
MITM	SSL, encryption, Intrusion Detection System	Yes	Yes	Yes
MITC	MFA, Data encryption, CASB	Yes	Yes	No
DoS	Intrusion Detection/Prevention System, Resource scaling, Hidden resources	Yes	Yes	No
Malware Injection	Sanitize user input, Avoid dynamically generated SQL, Service instance integrity check	Yes	Yes	Yes
Authentication	Password	Yes	Yes	No

	standards, password hashing, authentication tokens			
Phishing	Pop-up blockers	N/A	N/A	N/A
Port Scanning	Firewalls, TCP wrappers, Packet count	Yes	Yes	Yes
Cross-VM	Firewalls, Encryption/Decryption protocols	Yes	Yes	Yes
VM Rollback	Suspend and Resume	N/A	N/A	N/A
VM Escape	VM isolation, Monitoring hypervisor	N/A	N/A	N/A

Table 2: Software solutions

While at first glance it may seem like all three software options are equal in terms of cloud security, this may not be necessarily true as we are not privy to many details regarding these software suppliers internal processes to guarantee security. From the data made publicly available ownCloud seems to have a strong emphasis on security, both for the developers who contribute to this open-source project as well as having detailed security instructions in place for the end users who might make use of their products. This helps the cloud server to be as secure as possible during day-to-day use.

FileCloud was also notable in that they implement all the security features present in the other two, and more. Also, while the other two software services may limit certain security measures to higher paying customers (such as Two-Factor Authentication) NextCloud includes it in all of its software packages. This has the downside of coming

at a higher cost as there is no free option to FileCloud and the annual costs are the highest of the three.

PowerFolder has the advantage of being the most affordable of the three softwares we analysed, as well as having a free option. However, there are many security features which they limit to paying customers so a free version of this software wouldn't be sufficient for the needs of an institution that handles highly confidential information, such as the School of Applied Informatics.

5 - Conclusions

We have presented our study on the current state of cloud computing security taken from recent international literature.

Chapter 2 presents an overview of cloud computing architecture and security. Section 2.1 consite of a definition for cloud computing, it's different service levels and models, used as a reference throughout the remainder of the research. Section 2.2 presented an overview of the current security standards and vulnerabilities throughout the different models of cloud computing. Finally, Section 2.3 presented some solutions to each of the issues which were stated.

Chapter 3 looked at three cloud data storage enterprise softwares. These three softwares are presented in Sections 3.1, 3.2 and 3.3. We contrasted their currently implemented security solutions to those analysed in the previous chapter. Possible security breaches were pointed out.

Chapter 4 presents three of the most critical and notable attacks against cloud computing architectures. This chapter analysed the attacks' definition, the security vulnerabilities they seek to exploit and how to safeguard against them. We contrasted the countermeasures proposed by recent literature to those implemented by the cloud data storage enterprise softwares analysed previously in Chapter 3. Section 4.1 of this chapter presents man-in-the-cloud attacks, Section 4.2 distributed-denial-of-service attacks, and finally Section 4.3 malware injection attacks.

The analysis in this work could be used as a blueprint should the need arise to implement a cloud server for the School of Applied Informatics, as we analyzed in our motivation in Chapter 1. The nature of these softwares means that a server could be hosted either completely online or make use of the hardware already in place in the

school, and in this way could the extensive and important databases be migrated into the cloud. The annual sum for 50 users, which should meet the needs of the schools faculty and staff, surely must be far lesser than the cost required for regular maintenance and hardware replacement for the physical servers currently in place. Implementing any of the cloud data storage softwares analysed in this paper would mean easy and consistent access to school data as well as the practicality of secure and confidential file sharing between faculty members. Given this scenario, a proposal of how to best implement a cloud architecture for the school, studying and taking into account existing infrastructure and faculty opinion, could be an interesting avenue of future research.

5.1 Limitations

Due to the critical nature of the attacks analysed in Chapter 4, as well as legal constraints surrounding the cloud data storage enterprise softwares, we were not able to carry out any of the attacks ourselves in an ethical hacking endeavor. Penetration testing against these attacks would be an interesting way to both analyse and safeguard the cloud softwares against these attacks.

5.2 Future work

It is evident from our research and analysis that given the widespread adoption of the cloud, the security issues presented in recent literature must be addressed thoroughly. Therefore, enrichment of the existing solution techniques as well as more innovative approaches seeking to mitigate these problems are needed. Though Cloud Computing is an ever more popular software solution, it is still in its infancy, and its widespread adoption will rely heavily on how the ever increasing security concerns will be addressed in the upcoming days.

References

ALHENAKI, Lubna; ALWATBAN, Alaa; ALAMRI, Bashaer; Alarifi, Noof. **A Survey on the Security of Cloud Computing**, 2019. 2nd International Conference on Computer Applications & Information Security *(ICCAIS)*. Available at https://ieeexplore.ieee.org/abstract/document/8769497, access on 10 Dec, 2019.

BAKR, Ahmed; AHMED, Abd El-Aziz; HEFNY, Hesham. A Survey on Mitigation Techniques Against DDoS Attacks on Cloud Computing Architecture. **Journal of Advanced Science**. 28. 187-200. 2019. Available at: https://www.researchgate.net/publication/336923078_A_Survey_on_Mitigation_Techniques_Against_DDoS_Attacks_on_Cloud_Computing_Architecture, access on 02 of Dec, 2019.

BASESCU, Cristina et al. Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies. **2011 IEEE International Conference on Advanced Information Networking and Applications**. Singapore, IEEE, pp. 459-466, 2011.DOI: 10.1109/AINA.2011.61. Available at: https://ieeexplore.ieee.org/document/5763418, access on 12 of Oct, 2019.

BAZM, Mohammad-Mahdi; LACOSTE, Marc; SÜDHOLT, Mario; MENAUD, Jean-Marc. **Side Channels in the Cloud: Isolation Challenges, Attacks, and Countermeasures**, 2017. Available at https://hal.inria.fr/hal-01591808/document access on 13 Dec, 2019.

BEHAL, Sunny; KUMAR, Krishan. Characterization and Comparison of DDoS Attack Tools and Traffic Generators - A Review. **International Journal of Network Security**, 19(3):383–393, 2017. DOI: 10.6633/IJNS.201703. Available at: http://ijns.jalaxy.com.tw/contents/ijns-v19-n3/ijns-2017-v19-n3-p383-393.pdf, accessed on 02 of Dec, 2019.

CHAWKI, El; AHMED, Asimi; TBATOU, Zakariae. **IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors,** 2018. Procedia Computer Science. Available at https://www.sciencedirect.com/science/article/pii/S1877050918311451 access on 15 of Dec, 2019.

CHOI, Junho et al. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. **Soft Computing,** 18, pages 1697–1703, 2014. DOI: 10.1007/s00500-014-1250-8. Available at: https://www.researchgate.net/publication/271681680_A_method_of_DDoS_attack_detection_using_HTTP_packet_pattern_and_rule_engine_in_cloud_computing_environment. Accessed on 02 of Dec, 2019.

CHOUHAN, Priyanka; SINGH, Rajendra. Security Attacks on Cloud Computing With Possible Solution. **Journal of Advanced Research in Computer Science and Software Engineering.** India. IJARCSSE. Volume 6, Issue 1, 2016. Available at: https://pdfs.semanticscholar.org/2478/15a9f8439c8a61302c4e7de45ae19b1a6cc5.pdf, access on 05, Dec, 2019.

DEVI, T.; GANESA, R. **TELKOMNIKA Indonesian Journal of Electrical Engineering,** Vol. 15, No. 1, pp. 151 - 161, July 2015, DOI: 10.11591/telkomnika.v15i1.8073. Available at: https://pdfs.semanticscholar.org/4734/15b4c0ed79a629fc8b3424c9936db9583e77.pdf, access on 06 of Oct, 2019.

DO, Jeong-Min; SONG, You-Jin; PARK, Namje. Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments. **Proceedings of the 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering,** South Korea, IEEE, p.248-251, May 23-25, 2011. DOI: 10.1109/CNSI.2011.34. Available at: https://www.academia.edu/1280978/Attribute_Based_Proxy_Re-encryption_for_Data_Confidentiality_in_Cloud_Computing_Environments, Access on 13 of Oct, 2019.

FERNANDEZ, Eduardo B; YOSHIOKA, Nobukazu; WASHIZAKI, Hironori. Cloud Access Security Broker (CASB): A pattern for secure access to cloud services. 2015. Available at: https://pdfs.semanticscholar.org/fecb/163673cb5f87a40826dec5b1b4a796b60e8a.pdf, access on 20 of Oct, 2019

FRANÇOIS, Jérôme el al. BotCloud: Detecting Botnets Using MapReduce. **2011 IEEE International Workshop on Information Forensics and Security.** Foz do Iguaçu, Brazil. IEEE, Paper #55. 2011. DOI: 10.1109/WIFS.2011.6123125. Available at: https://ieeexplore.ieee.org/document/6123125, access on 04 of Dec, 2019.

HAMEED, Sufian; KHAN, Hassan Ahmed. SDN Based Collaborative Scheme for Mitigation of DDoS Attacks. **Future Internet 10.** (2018) DOI: 10.3390/fi10030023 Available at: https://www.semanticscholar.org/paper/SDN-Based-Collaborative-Scheme-for-Mitigation-of-Hameed-Khan/d53ec2324ecd57cadddb7ae111020ade786e4c6f, access on 05 of

Dec, 2019.

HASHIZUME, Keiko et al. An analysis of security issues for cloud computing. **Journal of Internet Services and Applications** 4, 5 (2013), doi:10.1186/1869-0238-4-5. Available at: http://www.jisajournal.com/content/4/1/5, access on 03 of Oct, 2019.

ION, Mihaela; RUSSELLO, G.; CRISPO, B. Enforcing multi-user access policies to encrypted cloud databases. **2011 IEEE International Symposium on Policies for Distributed Systems and Networks,** Italy, IEEE, pp. 175-177. DOI: 10.1109/POLICY.2011.14 Available at: https://ieeexplore.ieee.org/document/5976820, access on 12 of Oct, 2019.

ISLAM, Tariqul.; MANIVANNAN, D.; ZEADALLY, Sherali. A Classification and Characterization of Security Threats in Cloud Computing. **International Journal Of Next-generation Computing.** 2016. Available at: https://www.researchgate.net/publication/308172311_A_Classification_and_Characterization_of_Security_Threats_in_Cloud_Computing, access on 04 of Dec, 2019.

JABIR, R. M. et al. Analysis of cloud computing attacks and countermeasures, **2016 18th International Conference on Advanced Communication Technology (ICACT),** Pyeongchang, South Korea, IEEE, pp. 1-1. 2016. DOI: 10.1109/ICACT.2016.7423295. Available at https://ieeexplore.ieee.org/document/7423295, access on 18 of Oct, 2019.

KALAI VANI, Y.S; RANJANA, V. Anomaly Detection of DDOS Attacks Using Hadoop. In: Shetty N., Patnaik L., Nagaraj H., Hamsavath P., Nalini N. (eds) Emerging Research in Computing, Information, Communication and Applications. **Advances in Intelligent Systems and Computing**, vol 882. Springer, Singapore, 2019.

KHAN, Azaz; GILL, Nasib Singh. Review of Security Methods in Cloud Computing. **IJRAR- International Journal of Research and Analytical Reviews**. India, IJRAR. Vol.5, Issue 3. pp 2348-1269, 2018. Available at: http://ijrar.com/upload_issue/ijrar_issue_1405.pdf, access on 05 of Dec, 2019.

MAHJABIN, T. et al. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. **International Journal of Distributed Sensor Networks.** 2017. DOI:10.1177/1550147717741463. Available at: https://journals.sagepub.com/doi/full/10.1177/1550147717741463, access on 03 of Dec, 2019.

MEMARIAN, Reza; CONTI, Mauro; LEPPANEN, Ville. (2015). EyeCloud: A BotCloud Detection System. **2015 IEEE Trustcom/BigDataSE/ISPA**. Helsinki, Finland, pp 1067-1072, 2015. DOI: 10.1109/Trustcom2015.484. Available at: https://ieeexplore.ieee.org/document/7345392, access on 03 of Dec, 2019.

MORSY, Mohamed Al; GRUNDY, John; MULLER, Ingo. **An Analysis of the Cloud Computing Security Problem**, 2010. Available at: https://arxiv.org/ftp/arxiv/papers/1609/1609.01107.pdf, access on 06 of Oct, 2019.

NASEER, Amara; ZHIQUI, Huang; ALI, Awais. C**loud Computing Security Threats and Attacks with Their Mitigation Techniques**, 2017. Available at: https://www.researchgate.net/publication/322408253_Cloud_Computing_Security_Threats_and_Attacks_with_Their_Mitigation_Techniques access on 10 Dec, 2019

PATEL, Navneet Singh; REKHA, B.S. Software as a Service (SaaS): Security issues and Solutions. **International Journal of Computational Engineering Research (IJCER)**,Vol. 04, Issue 6, pp 2250 – 3005, June, 2014. Available at: http://www.ijceronline.com/papers/Vol4_issue06/version-2/J3602068071.pdf, access on 05 of Oct, 2019.

RAKOTONDRAVONY, N.; TAUBMANN, B.; MANDARAWI, W. *et al.* **Classifying malware attacks in IaaS cloud environments**, 2017. *J Cloud Comp* 6, 26. Available at https://link.springer.com/article/10.1186/s13677-017-0098-8 access on 13 of Dec, 2019.

SHAIKH, Asma. (2016). Attacks on cloud computing and its countermeasures. **2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)**. India, IEEE, pp 748-752. DOI: 10.1109/SCOPES.2016.7955539. 2016. Available at: https://ieeexplore.ieee.org/document/7955539, access on 05 of Dec, 2019.

SOMANI, Gaurav et al. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. **Computer Communications**, Eslevier, Vol.. 107, 2015. DOI: 10.1016/j.comcom.2017.03.010. Available at: https://www.researchgate.net/publication/288713585_DDoS_Attacks_in_Cloud_Computing_Issues_Taxonomy_and_Future_Directions, access on 18 of Oct, 2019.

SUBASHINI, S; and KAVITHA, V. **A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Net-Work and Computer Applications**, 2011. Available at https://www.sciencedirect.com/science/article/pii/S1084804510001281 access on 13 of Dec, 2019.

WANI, Aaqib; LONE, Zubair. **A Survey of Security Issues and Attacks in Cloud and their possible defences,** 2017. Available at https://www.researchgate.net/publication/321881866_A_Survey_of_Security_Issues_and_Attacks_in_Cloud_and_their_possible_defences access on 13 Dec, 2019.

WU, Hanquian et al. Network Security for virtual machine in Cloud Computing. **5th International conference on computer sciences and convergence information technology (ICCIT)**. Seoul, IEEE, pp. 18-21, 2010. DOI: 10.1109/ICCIT.2010.5711022. Available at: https://ieeexplore.ieee.org/document/5711022/citations#citations, access on 10 of Oct, 2019.

Wu, Jiang et al. **An Access Control Model for Preventing Virtual Machine Escape Attack**, 2017. Available at

https://www.researchgate.net/publication/317321419_An_Access_Control_Model_for_Preventing_Virtual_Machine_Escape_Attack, access on 25 Feb, 2020.

XIAOPENG, Gao; SUMEI, Wang; XIANQIN, Chen. VNSS: a Network Security sandbox for virtual Computing environment. **IEEE youth conference on information Computing and telecommunications (YCICT)**. Beijing, China, IEEE, pp 395–398, 2010. DOI: 10.1109/YCICT.2010.5713128, Available at: https://ieeexplore.ieee.org/document/5713128, access on 10 of Oct, 2019.

YANG, L.; ZHAO, H. DDoS Attack Identification and Defense Using SDN Based on Machine Learning Method, **15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN)**, Yichang, China, IEEE, 2018, pp. 174-178. DOI: 10.1109/I-SPAN.2018.00036. Available at: https://ieeexplore.ieee.org/document/8636336, access on 04 of Dec, 2019.

ZHANG, Xuan et al. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. **Proceedings of the 10th IEEE International Conference on Computer and Information Technology *(CIT 2010)*,** Bradford, UK, IEEE, pp. 1328-1334, June 29 - Jul 1, 2010. DOI: **10.1109/CIT.2010.501** Available at: https://ieeexplore.ieee.org/document/5577860/citations#citations, access on 10 of Oct, 2019.

Sites:

Cloud Computer Tutorial. **Gugu99.** 2019. Available at: https://www.guru99.com/cloud-computing-for-beginners.html, access on 25 of Oct, 2019

Cloud Computing. **Techonopedia.** Available at: https://www.techopedia.com/definition/2/cloud-computing, access on 20 of Aug, 2019.

Data Dispersion and Security In The Cloud, **CCSK GUIDE**, 2013. Available at: https://ccskguide.org/data-dispersion-and-security-in-the-cloud/, access on: 10 of Oct, 2019.

Developer_manual. **Owncloud.** Available at: https://doc.owncloud.org/server/8.1/developer_manual/, access on 18 of Oct, 2019.

FileCloud. 2019. Available at https://www.getfilecloud.com/ access on 13 of Dec, 2019.

FileCloud Security - Encryption In-Transit and At Rest. **Filecloud Codelathe.** Available at: https://www.getfilecloud.com/filecloud-encryption-in-transit-and-at-rest/, access on 19 of Oct, 2019.

FileCloud Security FAQ. **Filecloud Codelathe.** Available at: https://www.getfilecloud.com/FileCloud_Security_FAQ.pdf, access on 19 of Oct, 2019.

Forecast number of personal cloud storage consumers/users worldwide from 2014 to 2020 (in millions). **Statista.** 2016. Available at: https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/, access on: 10 of Nov, 2019.

Hardening and Security Guidance. **Owncloud.** 2018. Available at: https://doc.owncloud.org/server/10.3/admin_manual/configuration/server/harden_server.html, access on 19 of Oct, 2019.

Man in the Cloud (MITC) Attacks. **Imperva.** (2015) Available at: https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf, access on 03 of Dec, 2019.

OwnCloud. 2019. Available at https://owncloud.org/ access on 13 of Dec, 2019.

OwnCloud security development over the years. **Statuscode.** 2015. Available at: https://statuscode.ch/2015/09/ownCloud-security-development-over-the-years, access on 11 of Oct, 2019.

PowerFolder. 2019. Available at https://www.powerfolder.com/ access on 13 of Dec, 2019.

PRESSLEY, Alix. Best Cloud Advice to Protect Against a 'Man in the Cloud' Attack. **Intelligentciso**, 2019. Available at: https://www.intelligentciso.com/2019/03/14/protecting-against-a-man-in-the-cloud-mitc-attack/, access in 3 of Dec, 2019.

Security Advisories. **Owncloud.** 2019. Available at: https://owncloud.org/security/advisories/, access on 18 of Oct, 2019.

Security Guidelines. **Owncloud.** Available at: https://doc.owncloud.org/server/8.1/developer_manual/general/security.html, access on 10 of Nov, 2019.

Security Information. **Powerfolder.** 2019. Available at: https://powerfolder.atlassian.net/wiki/spaces/PF/pages/301834/Security+Information, access on 20 of Oct, 2019

Security work going on in ownCloud. **Statuscode.** 2015. Available at: (https://statuscode.ch/2015/05/security-and-owncloud-8.1/#new-security-guidance-and-tips--tricks, access on 15 of Oct, 2019.

WATTS, Stephen; RAZA, Muhamaad. SaaS vc PaaS vs IaaS: What's The Difference and How To Choose. **BMC Blogs.** 2019. Available at: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/, access on 25 of Oct, 2019.

What is a Denial-of-Service (DoS) Attacks? **Cloudfare.** 2020. Available at: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/, access on 25 of Feb, 2020.

What is Platform-as-a-Service (PaaS)? **Cloudfare.** 2019. Available at: https://www.cloudflare.com/learning/serverless/glossary/platform-as-a-service-paas/, access on 22 of Sept, 2019.

Man in the middle (MITM attack). **Imperva.** 2020. Available at: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ access on 25 of Feb, 2020.