Bachelor's thesis Bachelor of Engineering, Information and Communications Technology 2021

Prabin Pandey

SECURITY ATTACKS IN CLOUD COMPUTING



BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering, Information and Communication Technology

2021 | 45

Prabin Pandey

SECURITY ATTACKS IN CLOUD COMPUTING

This thesis discusses the major types of cybersecurity attacks. In particular, it discusses the essential process, needs, and a secure protocol that can be easily understood by beginners or those who are interested in using cloud computing as their daily services to counter potential network threats. The thesis deliberates the concept of network vulnerabilities for the early prevention from attack and suggests few mitigation techniques. The information provided in the given thesis has been amassed with a thorough secondary data collection and research techniques that demonstrated the majority of technologically dependent corporations and security experts who are aware of the potential cybersecurity threats. The conclusion of this thesis conveys ideas on different types of potential threats to cloud computing services based on data collected during 2020. The open data published in 2020 can be used by the reader to understand the potential cybersecurity threats in order to apply strategies for countermeasures in the coming future.

KEYWORDS:

Cloud Services, Cloud Security Attacks, Cloud Security Measures, Cloud Security Prevention

CONTENTS

LIST OF ABBREVIATIONS	5
1 INTRODUCTION	6
1.1 Background	6
1.2 Literature Review	6
1.3 Aim & Objectives	6
1.4 Problem Statement	7
2 OVERVIEW OF SECURITY ISSUES IN CLOUD COMPUTING	8
2.1 Cloud Computing Security threats	9
3 TYPES OF SECURITY ATTACKS	12
3.1 SaaS Level	13
3.1.1 Data Security	13
3.1.2 Data security over the cloud	13
3.1.3 Data Segregation	14
3.1.4 Data Breaches	14
3.2 PaaS Level	14
3.2.1 Data Location	14
3.2.2 Privilege Access	14
3.3 laaS Level	14
3.3.1 SLA or Service Level Agreement	15
3.3.2 Destributed Denail of Service	15
3.3.3 Man in the Middle	15
3.3.4 DNS Security	15
3.4 Classification of Cloud Security Attacks	15
3.4.1 Internal Attack	16
3.4.2 External Attack	17
3.5 Purpose of Cloud Security Attacks and Exploitation:	17
4 SECURITY THREATS IN CLOUD COMPUTING	19
4.1 Data Breaches	20
4.2 Misconfigurations	21
4.3 Malware, spyware, and viruses	22
4.4 Trojans	23

5 CLOUD SECURITY MEASURES AND PREVENTIVE METHODS	25
5.1 Cloud security measures	25
5.1.1 Cyber Security in Public	25
5.1.2 Cyber Security Concerns	25
5.1.3 The benefit of Cloud-Based Secure System	26
5.1.4 Cloud Provider Criteria & Preferences	26
5.1.5 Cloud Solution Criteria Based on Native vs Independent Cloud Security	
Solutions	26
5.2 Cloud security preventive methods	27
5.2.1 Strengthen Access Control	27
5.2.2 Multi-Factor Authentication:	28
5.2.3 Stronger Password	28
5.2.4 Active Surveillance	29
5.2.5 Data Integrity	29
5.2.6 Data Encryption	29
6 DISCUSSION	30
7 CONCLUSION	32
REFERENCES	34

FIGURES

Figure 1. Security Issues in the Cloud Computing.	8
Figure 2. Types of Security Attacks.	12
Figure 3. Classification of Cloud Security Issues.	16
Figure 4. Purpose of Cloud Security Attack & Exploitation (Tadapaneni, 2020).	18
Figure 5. Percentage of Organization Concerned about the Cloud Security	
(Schulze,2020).	19
Figure 6. Percentage of Biggest Cloud Security (Schulze, 2020).	20
Figure 7. Biggest Cloud Security Threats (Schulze, 2020).	22
Figure 8. Malware distribution (BullGuard, n.d.).	23
Figure 9. Trojan Horse Malware (Imperva, n. d.).	24
Figure 10. Cloud Computing Risk Mitigation and Prevention Techniques (Ali, Wood-	-
Harper, & Ramlogan 2020).	27
Figure 11. Factors for Strengthening Access Control (Shibli at al., 2014).	28
Figure 12. Cloud Migration Security Need (Schulze, 2020).	30

LIST OF ABBREVIATIONS

Distributed Denial of Services DDoS laaS PaaS SaaS

Infrastructure as a Service Platform as a Service Software as a Service

1 INTRODUCTION

1.1 Background

Cybercrime and attacks are becoming a common occurrence in the present technological era. Without proper prevention being assured against those attacks, it is quite ambitious for an organization to integrate cloud computing services. According to Milkovich (2020), 95% of cybersecurity breaches are triggered by human faults, and overall, 88% of the organization worldwide experienced a spear-phishing attack in 2019. With a drastic upsurge in attacks and exploitation in Cloud Computing-dependent organizations, it is essential to understand and adopt preventive measures to counter the potential threats that may come along the way. Some of the most common and troublesome network exploitations include DDoS Phishing, Brute Force, Man in the Middle, and SQL Injections that can have a significant impact on organizations with weak network configurations.

1.2 Literature Review

The thesis provides information regarding various cybersecurity attacks and their impact on the organization along with the mitigation strategies. The literature review in this thesis has been carried out with a proper assessment of secondary research and data collection method that has been implemented ethically. The literature review has been conducted using several internet resources that are legit and reliable such as "Cyber Security Threats, Challenges & Defense Mechanism in Cloud Computing", "Cloud Computing Security Challenges" and "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques.

1.3 Aim & Objectives

This thesis aims to illustrate various existing cyber and network threats that can be vulnerable for any business that operates through a cloud computing server. The primary objectives of this study are as follows:

- To research cloud computing, cyber-attacks, and the reasons for cyberattacks.
- To study how cyber attacks could be prevented using various mitigation tools and techniques.
- To elaborate on different types of cyberattacks vulnerabilities of cloud computing systems.
- To provide information regarding how cyberattacks can occur in an organization when adopting cloud computing.
- To research most potential mitigation techniques and countermeasures for cyber attacks prevention.

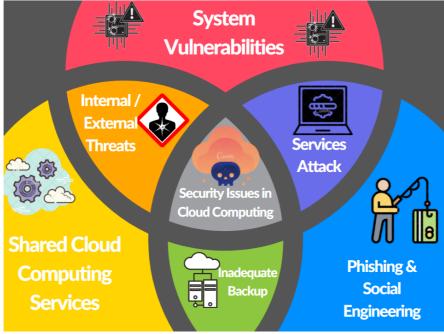
1.4 Problem Statement

The implementation of cloud computing and the digitalized system is the most common business trend that various organizations in today's time have implemented. However, several organizations implementing cloud computing solutions are generally unaware of potential hazards that can be devastating when an attacker breaks through the system. Most organizations are implementing weak physical and logical security for cloud computing in today's time. In order to tackle those, organizations need to be aware of potential network hazards and implement countermeasures.

2 OVERVIEW OF SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing security refers to securing the cloud computing environment against malicious and unauthorized access and the usage of services made available through the use of internet technologies (Tadapani, 2020). The types of security issues that can occur while using cloud computing services are internal/external threats, shared cloud computing services, inadequate backups, phishing, and social engineering, service attacks, and system vulnerabilities, as shown in Fig. 1 below. The exact initiation of cloud computing could be traced back to the mid-90s, and the earliest cloud computing implementor were Amazon and Ali Baba.

The increasing dependability of cloud computing for an organization has also enhanced the necessity to protect cloud-driven services with secure parameters that can protect the data available on the internet (Jathanna & Jagli 2017). The utilization and dependability in Cloud Computing services have offered the users greater reliability, massive scalability and have provided an economical cost of business expansion. Cloud computing technologies have added capabilities to major corporations to not only automate their daily business processes and requirements but also to create an easily accessible means of control using an



internet connection.

According to the analysis performed by Hashizume, Rosado, Fernandez-Medina, and Fernandez, (2013), cloud computing is a flexible and cost-effective method for daily business operations for the majority of organizations. The researchers also discussed about securing data in cloud computing, compliance, and its protection from exploitation (Hashizume et al., 2013). This thesis depicts major Figure 1. Security Issues in the Cloud Computing.

vulnerabilities and challenges in cloud computing such as "Cloud Storage Misconfiguration", "Insecure APIs" and "Theft of Intellectual Property" while implementing Cloud Computing services for any organization.

2.1 Cloud Computing Security threats

Cloud computing security threats include:

Lock-In Vendor is a condition that arises in cloud computing when a client is dependent on a single cloud provider, and a problem of inflexibility arises in the future. A lock-in vendor is an issue that lacks easy mobilization of the services or transferring of online services between different service providers and vendors (Opara-Martins, Justice, Reza, & Feng, 2018).

Loss of Governance is an issue related to cloud computing that occurs during the business migration from traditional on-premises IT infrastructure to cloud services without suitable governance policies, understanding, and implementations (Khalil, Fernandez, & Fautrero, 2016).

Compliance Challenges are legal and ethical problems that may arise during the implementation of cloud computing solutions for any corporation that follows the Health Insurance Portability and Accountability Act of 1996 or HIPAA to protect the privacy and security of specific health information (Yimam & Fernandez, 2016).

Supply Chain Failure is an issue related to the fulfillment of the supply chain after the implementation of Cloud Computing services. Because of the increased user orders through the internet connection, it can create a chance of degrading the goodwill with their customers (Aviles, 2015).

Technical Issues in cloud computing are related to the issues generated by the lack of technical fulfillments, such as inadequate computer systems and low user bandwidth that delays smooth business operations (Khan & Alam, 2017).

Malicious Insiders are another issue in cloud computing that may arise from the carelessness and minor faults of employees of the organization that can allow attackers and exploiters a chance to break down the system and perform unauthorized access (Saxena et al., 2020).

Shared Technology Cloud Services is a common type of cloud computing issue that occurs when a connection deployed on the internet is shared and made accessible to certain authorized parties that enhances the chances of exposure of sensitive data to the hackers and attackers (Pradhan, 2012).

Encryption of the data and information that are held or deployed through cloud computing technology needs to be made secure from a complex set of cryptography and encryption algorithms to protect the data even in cases of placed in unauthorized hands (Dharmakeerthi, 2020). Having weak or volatile encryption may also lead to issues in cloud computing.

Multi-Tenancy can be referred to as shared hosting, where a single software instance projects multiple distinct user groups, and various customers are distributed with necessary server resources (Aljahdali, Townend, & Xu, 2013).

Resource and Service Management after the deployment of cloud computing services can be quite complex to handle due to the increasing number of users

and queries that are made online and can be difficult for businesses that are new to cloud computing technology (Bendechache at al., 2020).

Services Level Agreements (SLA) is an agreement that is performed between cloud service providers to recognize the fulfillment of standards. An improper Services Level Agreements (SLA) lead toward a poor level of cloud computing services leading toward business backlashes (Patrick & Satyanarayana, 2020).

Denial of Service Attacks (DoS) is an attack that is a common threat for the computing services that are held online, which is generally carried out by injecting a huge unmanageable load of ping connections request directed from a different machine. DoS generally collapse the system with ping requests that are out of the cloud computing withstanding capacity (Srinivasan at al., 2019). These requests are used to offer the users cloud computing services for usability, management, and interaction with the system that needs to be properly provisioned, managed, orchestrate, and monitored to avoid cyber threats and exploitations (Odun-Ayo at al., 2018).

Data Loss or Leakage is an issue related to cloud computing implementation for businesses that require proper encryption and protocol assignments to avoid hackers and data loss during the communication made using internet connections (Tahboub & Saleh 2014).

The Data integrity refers to the reliability and trustworthiness of data throughout its lifecycle. Data integrity of the data held, used, or manipulated in any means should not be accessed by unauthorized personnel. Data Integrity is essential in cloud computing to supply different cloud computing services like PaaS, SaaS, and IaaS.

Natural Disasters and Availability can be devastating for a corporation that is only dependent on a single system that lacks the integration of a backup server, potentially leading to unintentional loss of crucial data and information (Ujjwal at al., 2019).

Loss of Back up creates a serious consequence for the business held in a cloud environment that led toward loss of previously saved data that can be countered by setting up additional standby backup servers in case of emergencies (Jan at al., 2020).

Data Transfer Bottlenecks refers to the bandwidth to and from the cloud provider in Cloud Computing. As cloud computing dynamically helps in creating a diversified business network and as a result, a latency problem can arise based on the number of hops required for the data transmission (Ibidunmoye,2016).

Interoperability in cloud computing is aimed at creating public and private cloud connections more secure and for a smooth link of communication. The main motive of interoperability is the ability of a computer system deployed in the cloud to securely exchange and make use of the information shared via an internet connection (Bouzerzour, Ghazouani, and Slimani, 2020).

Legal Jurisdiction issues regarding cloud computing could arise mainly from two aspects, geo-location and application served by cloud providers, including the laws and regulations that are followed in case of lawsuit file. For a business to implement cloud computing services, the organization needs to follow the regulations and protocols defined by the legal jurisdiction regarding the data usability and its deployment in the cloud (Hourani & Abdallah, 2018).

Data Privacy & Protection reflects the security of not only the data that has been stored and used in the offline system but also the data that has been hosted over the cloud for which the corporation needs to follow the jurisdiction and needs to fulfill the data protection and encryption criteria to counter huge compensation due to data breach (Shankarwar & Pawar, 2015).

Licensing Risk can be more troublesome in the IAAS and PAAS level of cloud computing as the users are not responsible for the management or control of the infrastructures, whereas certain privileges are provided in the cloud-deployed services. Most popular vendors such as Amazon and other cloud-based corporations follow a strict license to comply with the standards for minimal risk during licensing online services (Neicu at al., 2020).

Subpoena refers to compliance that is mandatory in cloud computing to secure the exchange of information via internet connection unless an encryption key is willingly shared between parties in the communication. The users using cloud computing services and involved in litigation must respond to the subpoena (O'Keeffe at al., 2020).

E-Discovery issues can create a selection in the wrong vendor that can be catastrophic for users for sharing their information when using the cloud service because it is essential to perform a proper eDiscovery for appropriate vendor selection, proper security insurance, and entering in a service agreement (Lee at al., 2013).

3 TYPES OF SECURITY ATTACKS

The initiation and integration of cloud computing services are copiously implemented by most of the corporations, which have also triggered the necessity to protect the cloud-deployed system from various types of network attacks like Distributed Denial of Service (DDoS), Man in the Middle, Brute Force, Data Breaches. The main objective for performing a cyber-attack in a cloud network or internet is to gather precise data and information that are kept under strict authorization requirements and authentications (Chou, 2020). The general attack vectors for cloud computing are to make access to the system to control and manipulate the cloud services and cause serious damages to the users utilizing the cloud platforms. The main intentions of the attacks include exploiting vulnerabilities and potential loopholes in the cloud system, theft of user's Intellectual Properties, and perform a malicious insider. The general classifications of Cloud Computing Services can be categorized as Software as a Service (SaaS) level, Platform as a Service (PaaS) level, and Infrastructure as a Service (laaS) level, which refers to using the software as service, platform as a service and infrastructure as a service. The main functionalities of SaaS level, laaS level, and PaaS level are to serve and handle cloud server with effective real-time system's operations and processing of information which mainly varies on software-based, infrastructure-based, and platform-based. Cloud Computing security attacks can be categorized based on the SaaS, PaaS, and IaaS which has been presented in Figure 3.

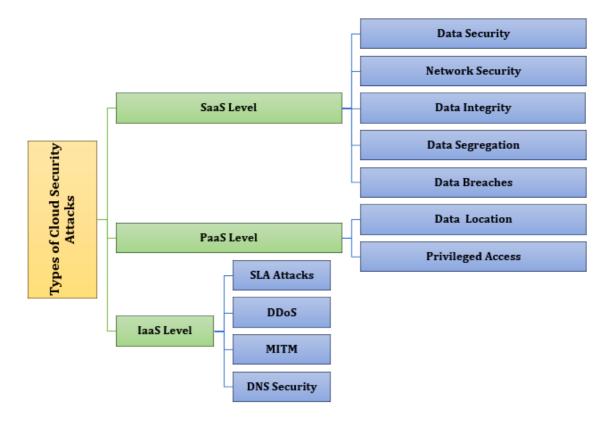


Figure 2. Types of Security Attacks.

The most common types of cloud security attacks can be categorized as shown in figure 3, whereas each of these attacks varies based on mediums, storage locations, communications, port numbers, etc. These cloud security threats and attacks have been segregated and explained briefly in the latter part.

3.1 SaaS Level

SaaS is a software licensing and delivery model which is made available through a third party with the use of internet technology that is licensed based on subscription made. Infrastructure as a Service or Hardware as a Service is one of the layers of cloud computing platform that serve a user with the capability to outsource their IT infrastructure overcloud (Rani & Ranjan, 2014). PaaS is a layer of cloud computing that is mainly used to supply the developer with a platform for the design and development of the application and system over the cloud. SaaS or even referred to as on-demand software is a level of cloud computing where software is licensed based on the subscription that is centrally hosted. The most effective trend of data protection over the cloud is data encryptions, whereas other substantial means of a data breach at the SaaS level could be phishing and malware attacks that could be used for stealing user's credentials. The consumer utilizing SaaS level of cloud services requires to understand different types of network attacks and threats, including their potential benefit and losses if encountered in the online system(Rani & Ranjan, 2014). The most common types of Cloud Security attacks existing at the SaaS level have been briefly explained below.

3.1.1 Data Security

Data security issues are a providential situation in a case when it is kept online or based on a real-time system hosted in the cloud for which data encryptions and protection against malware or protocols need to be followed for prevention of Intellectual Property Theft (Jathanna & Jagli 2017).

3.1.2 Data security over the cloud

Some of the basic standards for proper data security over the cloud is by creating permissions and privilege to read and write the particular data only by a specific individual. Most of the common network security issues in SaaS are, it lacks effective control and access to the sensitive data and inability to monitor the data in transit to or from the cloud applications (Aljumah & Ahanger, 2020).

3.1.3 Data Segregation

Due to poor monitoring over data in transit to and from cloud applications that Data Segregation could be quite complex work for the deployment of sensitive information over the cloud for which the best method of prevention is implementing powerful encryption in the data (Majeed, 2020)

3.1.4 Data Breaches

The data encryption could potentially help to counter the Data Breaches. It could be less accessible unless decrypted, even if the data is already in the hands of an unauthorized individual.

3.2 PaaS Level

PaaS or application platform as a service is based on cloud computing which offers the customer an application platform to design, develop, operate and manage cloud computing services. PaaS major limitation includes Data Security, Integration Vendor Lock-in, Customization to Legacy Systems, and runtime issues whereas some of the PaaS level threats have been summarized below.

3.2.1 Data Location

Data Location has become the common trend of cloud security issues in cases of PaaS, IaaS, and SaaS for which effective data encryption and protection against malware is essential.

3.2.2 Privilege Access

Privilege Access and proper access control protocols are essentially required for the protection of data that has been communicating through an online system. Most of the common trends to creating a strong system can be done by creating a complex set of passwords with strong encryptions mechanisms under well-supervised real-time monitoring and threat analysis (Blum, 2020).

3.3 laaS Level

laaS can be referred to as an online service that provides high-level APIs to classify different low-level details from an underlying network infrastructure like

physical computing resources, data partitioning, locations, security, backup, and scaling. The most common type of laaS threats has been presented below in brief.

3.3.1 SLA or Service Level Agreement

SLA or Service Level Agreement is a crucial part of a DDoS defense that needs to be properly analyzed to create tight configurations and protocols that can help in countering the distributed denial of service attack (Patrick & Satyanarayana, 2020).

3.3.2 Destributed Denail of Service

Destributed Denail of Service (DDoS) can be threatful attack for cloud computing which sends an unhandled number of ping connection request into a single IP address that eventually hangs and collapse the system (Srinivasan at al., 2019).

3.3.3 Man in the Middle

Man in the Middle (MITM) is a type of eavesdropping attack where an attacker intercepts and interrupts an ongoing communication or data transfer which is a type of eavesdropping attack (Shakshuki, 2016).

3.3.4 DNS Security

DNS security or Domain Name System Security is essential to protect the DNS system that is particularly used in a particular IP network which generally provides the authentication for the origin of the DNS data to safeguard against attacks and data integrity protection (Aishwarya, Sannidhan, & Balaji, 2014).

3.4 Classification of Cloud Security Attacks

Some other cloud security threats have been presented below based on the attacks that originate from inside and outside the organization.

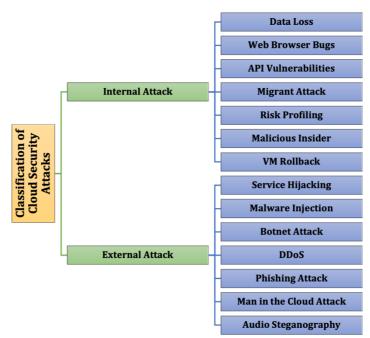


Figure 3. Classification of Cloud Security Issues.

3.4.1 Internal Attack

Internal Attacks generally occurred due to the carelessness of the employees and workers that are related to the particular organization. The most common reason for this type of attack is caused due to Employee Sabotage & Theft, Unauthorized Access by Employees, Weak Cyber Security Measure, and Unsafe Practices (Javaid,2013). Some of the attacks that occur due to insider's member of the organization have been presented below.

Data Loss generally happens which the hardware or software of the cloud system collapses and malfunctions that mostly happen by human errors. A data loss can occur when performing a data migration. Web Browser Bugs is another threat to cloud computing that can occur when the employees and workers of the organization utilize outdated applications and services (NSA, 2020). API Vulnerabilities can occur in cloud computing when the APIs lacks encryption, insecure endpoints, and weak authentication caused due to business logic flaws (Ariffin, Ibrahin, & Kasiram, 2020). The migrant attack is a multi-resource DoS attack on cloud virtual machine migration shames that compels a small set of compromised VMs to generate a useless resource consumption for misleading cloud monitoring (Chandrakala & Rao, 2018). Risk Profiling is essential for the insider of the organization to understand and access the measurement of the risk occurrence, impact, and future cure (Tadapaneni, 2020). Malicious Insiders can be former employees, contractors, or business associates who hold a privilege and authorization to the system and break down the system from within the organization by using malicious malware and computer virus (Duncan, Creese, & Goldsmith, 2012). VM Rollback is an attack where a compromised hypervisor operates a Virtual Machine from a previous snapshot without recognition and awareness of the users (Almutairy, 2019).

3.4.2 External Attack

The external attack generally penetrates and exploits the cloud system from the external influence like through the means of internet connections (Usman, Awwalu, & Kamil, 2016). Surging an external attack to the cloud system could be devastating and break down the system that could negatively impact the organization's daily business processes. Some of the external attacks could potentially occur a huge loss for the organization utilizing the cloud system. Service Hijacking can be a critical security threat for cloud computing services which can occur when unauthorized personnel grants access to the system over the cloud (Tirumala, Sathu, & Naidu, 2015). Malware Injection is another external threat to cloud computing that can occur when malware is injected into the organization's online system through various means and methods like process injections (Watson et al., 2015). Botnet Attack is similar to the DDoS attack, where a bot is automated for performing an attack in a specified target from huge numbers of a computer that potentially hangs and collapses the system (Anwar et al., 2014). A phishing Attack is another dreadful attack that creates a similarlooking application and tricks an authorized user with a fake application by fetching important information like the user's credentials and personal details (Basit at al., 2020). Man in the Cloud Attack is a vulnerable attack for cloud system which allows hackers and unknown parties to access as well as control the data and information that is stored in popular file synchronization services such as Google Drive and Dropbox (Jabir at al., 2016). Audio Steganography is a trending and vulnerable attack for a cloud-based system that can eavesdrop the data by attacking LAN that is hidden in an audio file format (Awadh, Hashim, & Hamoud, 2019).

3.5 Purpose of Cloud Security Attacks and Exploitation:

Cloud Malware Injection is performed to take control of a user's information that is kept in the cloud. Abuse of Cloud Services is a condition when an attacker gains access to the system or control of the file, which is generally performed by malicious users. Denial of Service is performed to shut down the system operating in a cloud-based system and making it inaccessible to the intended users. A Side-Channel Attack is performed for the extraction of the secrets from a chip or system.

A wrapping Attack is performed for injecting a fake element into a message structure to replace the invalid signature with a similar signature, whereas the fake one is processed by application logic. Man in Cloud Attack is performed with the main intention to gain access to its victim's account without the need to obtain compromised user's credentials. Insider Attack is performed to steal property or information for personal gain or even to benefit other competitors. Account or Service Hijack is performed to access the user's account credentials and hijack with unauthorized access or hijack to the cloud sessions. Spectre & Meltdown is performed for allowing arbitrary locations in an allocated memory of a program to be read which allows the process to read all memory in a cloud computing system. Advanced Persistent Threats (APTs) are performed to establish an illicit, long-term presence on a network for mining highly sensitive data.



Figure 4. Purpose of Cloud Security Attack & Exploitation (Tadapaneni, 2020).

4 SECURITY THREATS IN CLOUD COMPUTING

Even though the popularity of using cloud computing for most organizations is a common thing contextually while holding an online system in a secure parameter, but it has become one of the most important concerns at present. For the precise collection of a detailed piece from any research work, it is essential to understand the core priorities and protocols that are needed to be followed for maintaining the standards. Looking at the present cybersecurity progression and development particularly in the field of cloud computing, it is quite essential to understand a depth analysis of different challenges and negative aspects before migrating a corporation's business process to an online system.

The system migration from a traditional paper desk work is seamlessly complex and time consuming while transferring it to the cloud platform while some lesser when done from a data center. Even though there are numerous benefits for implementing a cloud system for an organization, it also increases the chances of exposure to a corporation's vital data and information. Similarly, the 2020 COVID 19 pandemic crisis led toward increased dependability on work from home, which eventually accelerated the business toward cloud computing migrations for keeping up with the target.

The data analysis and findings have been collected from the openly available research work conducted on Cloud Security Report by Cybersecurity Insiders which publishes precise statistical information regarding cloud computing security (Schulze, 2020).

How concerned are you about the security of public clouds?

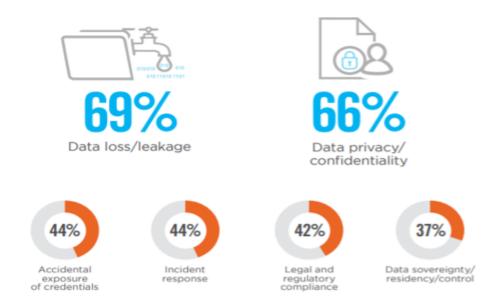


Figure 5. Percentage of Organization Concerned about the Cloud Security (Schulze,2020).

According to the survey conducted by Cybersecurity Insider shown in figure 5 above, the majority of the corporations that are extremely dependent on Cloud Computing is 33% and only 1% are not concerned about cloud computing security. On average, 42% of the majority of corporations are concerned about cloud security. The provided data shows how the highest percentages of the population are concerned about cloud security and its negative impact after exposure of information in an online system without prior security measure implementations. Security is always a key concern for a cloud computing solution to small to large-scale organizations. The statistical report depicts that 75% of the cybersecurity professionals are sure and are well concerned about the public cloud security which recently has increased in the previous year.

4.1 Data Breaches

The biggest cloud security concern for the majority of corporations is data loss or leakage occurrence in the corporation. The statistics published by Cyber Security Insiders, as shown in figure 7 above, reveals information that the biggest cybersecurity concerns for most of the organization are data leakage by 69% and data privacy confidentiality by 66%. Though the cloud computing service provider mostly implements a complex set of network protocol and cybersecurity measures to counter most of the potential threats being over the internet, where most of the time, the issues come from the final consumers or the user of the application. The data depicts that most of the users operating in the cloud computing system are most likely to responsible for leading toward 69% of data loss/ leakage and 66% of data privacy/ confidentiality issues.



What are your biggest cloud security concerns?

Figure 6. Percentage of Biggest Cloud Security (Schulze, 2020).

According to the statistic published by Cyber Security Insider shown in figure 6 depicts that the 44% majority of the corporation are concerned about accidental exposure of credentials and incident response, 42% are concerned about legal and regulatory compliance, and 37% are concerned about data sovereignty/residency and control.

4.2 Misconfigurations

The most common questions regarding which is the biggest security threat when using a cloud service are directly relatable to the most trending attacks and exploitations caused by unauthorized access, insecure interfaces, and APIs. The statistics collected by Cyber Security Insiders as shown in figure 7, shows that the highest chances of poor security conditions were triggered due to misconfiguration of the cloud platform and wrong setup, which is 68% which was in the third spot that could have been due to the development of complex application not easy to configure tightly. Similarly, the biggest changes of cloud security include unauthorized access which is by 58% and insecure interfaces or APIs includes 52%. Other security threats like Hijacking of accounts, Services, or Traffic were rated with 50%, External Sharing of Data by 43%, Malicious Insiders by 36%, Foreign State-Sponsored Cyber Attacks by 33%, and Denial of Service Attacks by 28%.



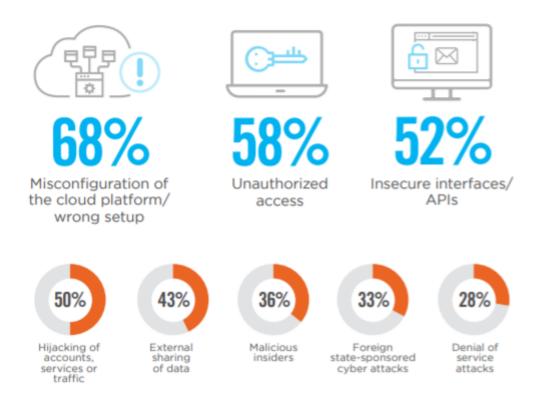


Figure 7. Biggest Cloud Security Threats (Schulze, 2020).

4.3 Malware, spyware, and viruses

Several kinds of macro viruses include a file infector that is liable to tunnel and the files that are executable and can outspread via a network that seeks benefit from the programs supporting macros. Furthermore, polymorphic viruses are able to alter their private code. These virus duplicates and encrypts themselves by altering the code and evade the antivirus detection. Besides, spyware is one of the types of malware that collects data about users secretly after it is injected into the user's device. The websites visited by the user along with the computer system's information and possible future attacks, can be detected by spyware. Malware is the collection of every malicious software that includes viruses with variability goals. Malware programs are primarily introduced to trick the victim into extracting their personal information for identity theft and steal their credit card and other financial information. Moreover, they tend to infect the victim device and utilize them for bitcoin mining and several crypto currencies. As shown in the figure 8, Malware distribution has been done in certain types such as Adware, Backdoor viruses, Spyware, Traditional viruses, and Trojans, etc.

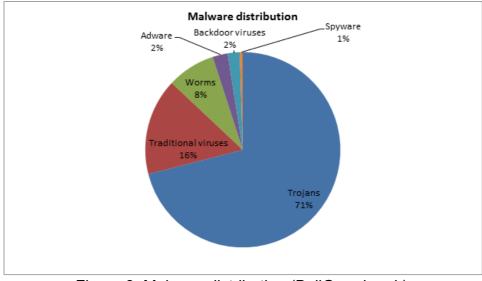


Figure 8. Malware distribution (BullGuard, n.d.).

4.4 Trojans

A Trojan is also known as a Trojan horse. It is a kind of software or malicious code, which seems legitimate but can also control the infected computer. Mainly, a Trojan is introduced for the disruption, damage, and steal or, in other words, impose harmful action on the network or data. A Trojan function like a bona fide application to trick the victim. It looks for the opportunity to deceive the victim into loading and executing the malware in the device. After the installation, a Trojan is liable to conduct the action it was intended for. However, a Trojan is not able to execute and duplicate itself. A user needs to execute Trojans. Backdoor, DDoS attack, downloader, fake AV, ransom, rootkit, info stealer, SMS, are some common types of Trojans. In the figure 9, proper operation for trojan horse malware is illustrated in steps.

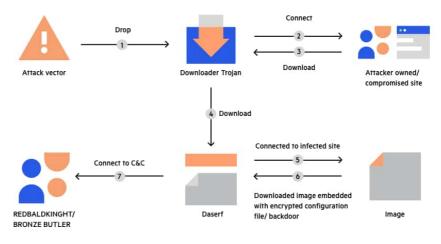


Figure 9. Trojan Horse Malware (Imperva, n. d.).

5 CLOUD SECURITY MEASURES AND PREVENTIVE METHODS

5.1 Cloud security measures

Cloud Security is effectively used as a technology and policy for strict manipulation of services in the online system. When comparing cloud security between public and on-premises systems, the cloud security in public can be vulnerable and prone to cyber-attacks. The most common reason for threats in cloud security is due to weak security systems and careless or inexperienced vulnerable insiders of the corporation that are relying on or is about to implement secure cloud security in public.

5.1.1 Cyber Security in Public

As most of the corporations that implement a cloud-based system require complex security along which is mostly considered by each organization that is deploying their cloud-based services to its consumer exposed in public. Cloud Computing can be categorized as Public Cloud, Private Cloud, and Hybrid Cloud. The public cloud refers to a model of cloud computing that is used to deliver the service to its consumer through the medium of the internet connection.

The private cloud refers to a cloud computing model that is generally designed to provide a wireless connection that is used for internal and a single organization. A hybrid cloud is a cloud-based approach that uses both public and private cloud systems for its consumers. Most of the corporations hold 38% of the workload in public and 41% in the private cloud, where the private cloud is used for crucial activities and slightly less vital work in the public cloud.

5.1.2 Cyber Security Concerns

For safe cloud computing practices, it is essential to understand the different cloud security concerns as approximately 70% of the global population operates using cloud computing technologies due to the benefit of flexibility, compliance, and compatibility to the general consumer.

According to the survey conducted by Cyber Security Insiders published information regarding the most potential cloud security concern are data loss/leakage (69%), data privacy (66%), data confidentiality (44%), accidental exposure of the credentials (44%), incident response (44%), legal and regulatory compliance (42%), data sovereignty (37%), residency (37%), and control (37%) (Schulze, 2020). Other different Cloud security Concern includes Data Breaches, Account Hijack, Insider Threats, Malware Injection, Cloud Services Abuse, Insecure APIs, Denial of Service Attacks, Insufficient Due Diligence, and Shared Vulnerabilities.

5.1.3 The benefit of Cloud-Based Secure System

The most potential benefit of a Cloud-Based Secure system can help in promoting a faster time for the service deployment to its consumers, save the budget required for the project, and helps in reducing efforts that are required for program's update and patches to the system. Other benefits of a Cloud-Based Secure System can provide the consumers with better visibility into the user activities and system behaviour. The data and workloads of each second in the corporation can be saved in the cloud or can be used to shift the data from one to another cloud system for meeting the cloud compliance expectations.

5.1.4 Cloud Provider Criteria & Preferences

Cloud Providers like Amazon, Azure, Google Cloud, Oracle Cloud, IBM Cloud, Rackspace, and Alibaba Cloud are considered the top 7 Cloud Computing Service Providers in the market. The most common questions while selecting a cloud provider is based on the cost for cybersecurity (63%), ease of deployments (53%), security tools & cloud-native (52%), and Deployments with Automation (52%), including other criteria like interoperability with an on-premises system (48%), policy customization (44%), integrate seamlessly with cloud platforms (44%) and multi-cloud support (42%) as extracted from the research work by Cyber Security Insiders among 653 Cyber Security Specialists.

The research and analytics performed by Cyber Security Insiders among 653 Cyber Security Specialists show that the majority of the corporation selected Amazon Web Service as their top target in comparison to cloud service providers that may vary due to the user preference.

5.1.5 Cloud Solution Criteria Based on Native vs Independent Cloud Security Solutions

The most important criteria based on the Native and Independent Cloud Security Solution are the cost required for a cloud-based security solution, ease of using the cloud-based system, user friendly, and well-integrated that is developed for ease in operation. Other Cloud Security Solutions include performance, quicker deployments, cloud vendor security, and reliability. A Native Cloud Security refers to the integrated cloud service which can be referred to as both platform and infrastructure security as well as continuous application security. The native cloud security solution is created for a microservice architecture whereas an independent cloud is created to serve a specialized purpose and cloud-enabled applications are made on a legacy infrastructure system and each module is dependent on the other.

5.2 Cloud security preventive methods

For a secure cloud computing services implementation for an organization, it is essential to understand different types of attack and their mitigation techniques that need to be implemented early for countering in the coming future as shown in figure 10. One of the most important standards for the migration of potential cloud computing threats is creating a signed agreement with the relevant parties before any casualties that can occur in the coming future. Other standard cloud computing threat mitigation techniques include limiting the user's access, research on a vulnerable aspect of the system, analyze the open port, and developing a proper incident response plan (Ali, Wood-Harper, & Ramlogan 2020).

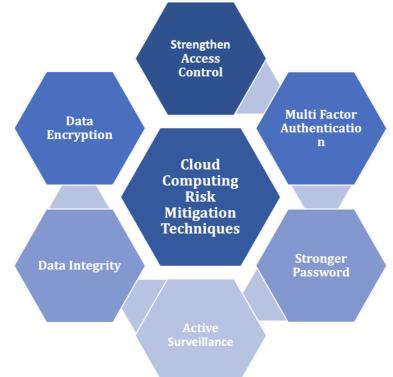


Figure 10. Cloud Computing Risk Mitigation and Prevention Techniques (Ali, Wood-Harper, & Ramlogan 2020).

5.2.1 Strengthen Access Control

To construct a secure cloud computing system, the security-relevant parties in the given organization need to evaluate the previous access control system properly and create a new set of access control that integrates the weak configuration to a stronger one (Shibli at al., 2014). The most common trends for strengthening access control are multifactor authentication, implementing stronger password policies, securing password files, restricting access to the system, and use of account lockout policies. The most common trends of strengthening access control have been presented in the figure 11 below.



Figure 11. Factors for Strengthening Access Control (Shibli at al., 2014).

5.2.2 Multi-Factor Authentication:

The use of Multi-Factor Authentication helps to verify the identity of the users based on cross-platform or another account that is linked for the authorized access to the system (Banyal, Jain. P, & Jain. V, 2013). The most common and traditional way of authentication is performed by using the account's username and password while the multi-factor authentication surpasses this system of authentication and allows the user to add multiple account addresses like Gmail, Mobile Number, and other open-source connection to verify whether the user is authentic or not which can help in countering the unauthorized access to the system.

5.2.3 Stronger Password

Another effective way to counter various cloud computing attacks like a brute force that can reduce the chances of attack through random keystrokes whereas the attacker can use the automation script to select the right character for the password fields (Brandao, 2018). Most of the sensitive account are hence allows

users to enter only several times like thrice at maximum for the protection of the cloud system from an attack like brute force.

5.2.4 Active Surveillance

Another effective way of protecting the cloud computing system is by performing active surveillance to the online system which involves monitoring the network traffic, including incoming and outgoing packets of data, and analysis of vulnerable ports that can leak sensitive information without awareness of the users (Gong, 2020). Active surveillance on the ports that are on inactive communications and each packet of data should be analyzed for cloud computing security and protection.

5.2.5 Data Integrity

The data which is held online on a cloud system requires to be properly protected from malware and attack with the need of encryption following a complex set of algorithms that can help in strengthening the file security even it falls in the wrong hand. Most of the corporations that are adopting cloud computing are utilizing a huge load of data and information from its customer as well as the insider employees for which the encryption of data is essentially required (Megouache, Zitouni, & Djoudi, 2020). Similarly, the sensitive data should be defined with a predefined set of permissions, and privilege should be provided to only authorized personnel.

5.2.6 Data Encryption

The data that has been used and stored by the corporation based on cloud computing service needs to be aware of the data encryption to preserve the data and its information integrity. A powerful set of data encryption conducted on sensitive data could help in preventing exposure of information in the wrong hand, even if it is already taken by unauthorized personnel (Megouache, Zitouni, & Djoudi, 2020). Moreover, the popular corporations based on cloud computing for the protection of the data take data security seriously and even utilizes their own complex set of encryption methods for making it almost impossible to decrypt the encryption key.

6 DISCUSSION

The terms cloud computing and cyber-attack are discussed in brief with the exploration of most of the terminologies related to them. The reason for Cyber Attacks and their types, anatomy, and method are also researched and understood. The steps included in the prevention of Cyber Attacks are also learned along with the mitigation tools and techniques. Furthermore, the vulnerability of the cyber-attacks to cloud computing systems are presented along with several methodologies and anatomy of distinct Cyber Attacks. Likewise, the process of adaption of cloud computing by Cyber Attackers is explained and the research on the highly potential mitigation and countermeasures for Cyber Attack preventions is conducted in this thesis.



When moving to the cloud, how do you handle your changing security needs?



The survey conducted by the CEO of Cyber Security Insiders shown in figure 12, delivers information regarding how to handle dynamic security needs while migrating to cloud-based services. It was observed that 61% of the population voted for the solution by providing training and certify the employees working in

the organization, while 58% voted for the use of native cloud provider security tools. Furthermore, the remaining cloud migration security needs were to hire a staff dedicated to cloud security by 34%, deploy security software from independent software vendors by 30%, and partner with a managed security services provider (MSSP) by 29%. Most of the corporations have implemented an approach that includes providing training to the employees and subordinates below the main presenter to convey the measures for cloud-based security, including schemes like providing certification to the IT staff.

7 CONCLUSION

The present context of cloud computing requires complex security and protection against different threats such as phishing and social engineering, shared cloud computing services, internal/external threats, system vulnerabilities, services attack, and inadequate backup. These threats have been discussed in this thesis, along with proper illustrations. Cloud computing services help online organizations to perform their business operation using a 24/7 available online system. Cloud computing services can be implemented in three major forms that are known as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service Platform as Service (PaaS), which have been illustrated in this thesis along with potential cloud security threats based on SaaS, laaS and Paas. Each of the attacks has been classified accordingly and organized in a hierarchical order to provide a in-depth understanding of cloud security attacks.

The major significance of the study work conducted in this thesis lies in that the thesis provides an overview of the top trending cloud security threats from peerreviewed sources during 2020 and real-time examples based on those trending cloud security threats. As per the critical assessment conducted through research, effective strategies for mitigating cloud security risk can be Data Encryption at REST, Two Factor Authentication, Eliminate Shared Accounts, insisting on a Well-Defined Shared Responsibility Model, and using Standardized Cloud Assessment. The use of data encryption at REST helps in minimizing the risk by ensuring data security which adds another layer of security to the data, which increases the requirement of a decryption key to access the particular data. Organizations compulsorily implement data encryption technology to maintain compliance with cybersecurity and governmental standards. The use of twofactor authentication can help in securing the cloud-based system and help in supporting the system with ease of use from an end-user perspective. Two-factor authentication has become the common compliance that is mandatory in the present cloud-based system. Most of the daily business operations of an organization are based on a common sharing cloud platform with proper credentials, which can create a loophole for the attacker.

This thesis has also discussed various network threats and hazards that could cause potential harm to the system. Moreover, the thesis has delivered information regarding the different types of attacks, their cause for origination, the anatomy of the attack, and mitigation techniques. The thesis only provides the reader with secondary knowledge and does not implement cybersecurity attacks for demonstration. The implementation of cloud computing and the digitalized system is regarded as one of the most needed business trends. Moreover, most of the organizations implementing cloud computing solutions are unaware of the potential hazards, which can be devastating when an attacker breaks through the system. Most corporations are implementing a weaker physical and logical security for cloud computing, for which the organization needs to be aware of the potential network hazard and implement countermeasures for the attack.

A secure Cloud-Based system can help in promoting a faster time for the service deployment to its consumers, saving the budget required for the project, and

reducing efforts that are required for program updates and patches to the system. A secure Cloud-Based System can also provide the consumers with better visibility into the user activities and system behaviour. The data and workload of each second in the corporation can be saved in the cloud or can be used to shift the data from one to another cloud system to meet the cloud compliance expectations.

Access control helps in providing physical and information security by restricting access to a place or sensitive resources that are only permitted to authorized personnel in certain circumstances and conditions. The development of a proper access control policy? promotes the cloud system with a restriction on different aspects, which most importantly helps in creating confidentiality, integrity, and accessibility among legitimate users. After the corporation's processes are migrated to the cloud, it is strictly necessary to monitor the online transactions, which need to be encrypted and protected against cybersecurity attacks and threats that could harm the system and eventually compensate the corporation hugely in the coming future. For proper identification of the network threat of a cloud-based system, it is essential to hire a penetration tester who regularly conducts penetration testing against the cloud-based system to find vulnerabilities and bug holes. The corporation which has already adopted a secure cloud-based solution or is on the way to implement one needs to be aware of the system its features, advantage, and disadvantages to comply with the system properly and take its full advantage. To increase the awareness of the employees and the users of the cloud-based system, each of the relevant individuals needs to participate in the security training where the basic and secure protocols are taught to the employees and users to counter chances of misconfigurations and potential cybersecurity threats in the coming future. (Aljumah & Ahanger, 2020)

REFERENCES

Aishwarya, C., Sannidhan, M. S., & Rajendran, B. (2014, December). DNS Security: Need and Role in the Context of Cloud Computing. In *2014 3rd International Conference on Eco-friendly Computing and Communication Systems* (pp. 229-232). IEEE.

Ali, M. B., Wood-Harper, T., & Ramlogan, R. (2020). A Framework Strategy to Overcome Trust Issues on Cloud Computing Adoption in Higher Education. In *Modern Principles, Practices, and Algorithms for Cloud Security* (pp. 162-183). IGI Global.

Aljahdali, H., Townend, P., & Xu, J. (2013, March). Enhancing multi-tenancy security in the cloud IaaS model over public deployment. In *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering* (pp. 385-390). IEEE.

Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. *IET Communications*, *14*(7), 1185-1191.

Almutairy, N. M. (2019). A taxonomy of virtualization security issues in cloud computing environments. *Indian Journal of Science and Technology*, 12(3), 1-19.

Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

Anwar, S., Zain, J. M., Zolkipli, F., & Inayat, Z. (2014). A review paper on botnet and botnet detection techniques in cloud computing. *Proceedings of the ISCI*, 28-29.

Ariffin, M. A. M., Ibrahim, M. F., & Kasiran, Z.(2020). API Vulnerabilities In Cloud Computing Platform: Attack And Detection. *In 2020 International Journal of Engineering Trends and Technology*(pp8-14).

Aviles, M. E. (2015). The impact of cloud computing in supply chain collaborative relationships, collaborative advantage and relational outcomes (Electronic Theses and Dissertations Graduate Studies, Georgia Southern University) retrieved from

https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=2312&c ontext=etd Awadh, W. A., Hashim, A. S., & Hamoud, A. (2019). A Review of Various Steganography Techniques in Cloud Computing. *University of Thi-Qar Journal of Science*, *7*(1), 113-119.

Banyal, R. K., Jain, P., & Jain, V. K. (2013, September). Multi-factor authentication framework for cloud computing. In *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation* (pp. 105-110). IEEE.

Banyal, R. K., Jain, P., & Jain, V. K. (2013, September). Multi-factor authentication framework for cloud computing. In *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation* (pp. 105-110). IEEE.

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 1-16.

Bendechache, M., Svorobej, S., Takako Endo, P., & Lynn, T. (2020). Simulating resource management across the cloud-to-thing continuum: A survey and future directions. *Future Internet*, *12*(6), 95.

Blum, D. (2020). Control Access with Minimal Drag on the Business. In *Rational Cybersecurity for Business* (pp. 227-257). Apress, Berkeley, CA.

Bouzerzour, N. E. H., Ghazouani, S., & Slimani, Y. (2020). A survey on the service interoperability in cloud computing: Client-centric and provider-centric perspectives. *Software: Practice and Experience*, *50*(7), 1025-1060.

Brandão, P. (2018). The Importance of Authentication and Encryption in cloud computing framework security.

BullGuard. (n.d.). A definition of malware. Available at: <u>https://www.bullguard.com/bullguard-security-center/pc-</u> <u>security/computer-threats/ Accessed: May 28 2021</u>

Chandrakala, N., & Rao, B. T. (2018). Migration of Virtual Machine to improve the Security of Cloud Computing. *International Journal of Electrical and Computer Engineering*, *8*(1), 210.

Dharmakeerthi, T. D. (2020) A Study on Secure File Storage in Cloud Computing using Cryptography (Sri Lanka Institute of Information Technology University, Western Province, Sri Lanka). Retrieved from <u>https://www.researchgate.net/profile/Thilina-</u> <u>Dharmakeerthi/publication/341508689 A Study on Secure File Storage in</u> <u>Cloud Computing using Cryptography April 2020/links/5ec4d77e92851c11a8</u> <u>77966c/A-Study-on-Secure-File-Storage-in-Cloud-Computing-using-Cryptography-April-2020.pdf</u>. Duncan, A. J., Creese, S., & Goldsmith, M. (2012, June). Insider attacks in cloud computing. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 857-862). IEEE.

Gong, M. (2020). *Cloud-Based System for Effective Surveillance and Control of COVID-19: Useful Experiences From Hubei, China.* Journal of Medical Internet Research, 22(4), 4-20.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 1-13.

Hourani, H., & Abdallah, M. (2018, July). Cloud computing: legal and security issues. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 13-16). IEEE.

Ibidunmoye, O. (2016). *Performance problem diagnosis in cloud infrastructures* (Doctoral dissertation, Department of Computing Science, Umeå University).

Imperva. (n.d). *What is a Trojan Virus*. Available at :<u>https://www.imperva.com/learn/application-security/trojans/</u><u>Accessed: May 15 2021</u>

Jabir, R. M., Khanji, S. I. R., Ahmad, L. A., Alfandi, O., & Said, H. (2016, January). Analysis of cloud computing attacks and countermeasures. In *2016 18th International Conference on Advanced Communication Technology (ICACT)* (pp. 117-123). IEEE.

Jan, S. U., Ghani, D., A Alshdadi, A., & Daud, A. (2020). Issues and challenges in cloud storage architecture: a survey. *, Issues and Challenges in Cloud Storage Architecture: A Survey.* Researchpedia Journal of Computing, Volume 1, Issue 1, Article 6, Pages 50–65, Jun 2020.Available at <u>https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630761</u> accessed: May 07 2021

Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. *International Journal of Engineering Research and Applications*, 7(6), 31-38.

Javaid, A. (2013). Top Threats to Cloud Computing Security.SSRN Electronic Journal.10.2139/ssrn.2325234

Khalil, S., Fernandez, V., & Fautrero, V. (2016, August). Cloud impact on IT governance. In *2016 IEEE 18th Conference on Business Informatics (CBI)* (Vol. 1, pp. 255-261). IEEE.

Khan, I. R., & Alam, M. (2017). Cloud Computing: Issues and Future Direction. *Global Sci-Tech*, *9*(1), 37-44.

Lee, T., Kim, H., Rhee, K. H., & Shin, U. S. (2013). Design and Implementation of E-Discovery as a Service based on Cloud Computing. *Computer Science and Information Systems*, *10*(2), 703-724.

Majeed, M. G. A. S. S. (2020). Data security in cloud computing. *Solid State Technology*, *63*(6), 7184-7193

Megouache, L., Zitouni, A., & Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. *Human-centric Computing and Information Sciences*, *10*, 1-20.

Megouache, L., Zitouni, A., & Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. *Human-centric Computing and Information Sciences*, *10*, 1-20.

Milkovich, D. (2020, December 23). *Cybint*. From Cybintsolutions: Available at : <u>https://www.cybintsolutions.com/cyber-security-facts-stats</u>. Accessed: May 13 2021

Neicu, A. I., Radu, A. C., Zaman, G., Stoica, I., & Răpan, F. (2020). Cloud Computing Usage in SMEs. An Empirical Study Based on SMEs Employees Perceptions. *Sustainability*, *12*(12), 4960.

O'Keeffe, D., Vranaki, A., Pasquier, T., & Eyers, D. (2020, April). Facilitating plausible deniability for cloud providers regarding tenants' activities using trusted execution. In 2020 IEEE International Conference on Cloud Engineering (IC2E) (pp. 59-65). IEEE.

Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018, July). Cloud computing architecture: A critical analysis. In 2018 18th international conference on computational science and applications (ICCSA) (pp. 1-7). IEEE.

Odun-Ayo, I., Geteloma, V., Falade, A., Oyom, P., & Toro-Abasi, W. (2019, December). A Systematic Mapping Study of Utility-Driven Models and Mechanisms for Interclouds or Federations. In *Journal of Physics: Conference Series* (Vol. 1378, No. 4, p. 042008). IOP Publishing.

Opara-Martins, Justice, Reza Sahandi, and Feng Tian. "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective." *Journal of Cloud Computing* 5, no. 1 (2016): 1-18.

Patrick, Z. P. G., & Satyanarayana, K. (2020). optimization of service level agreements (SLAS) within saas cloud it infrastructure. *Journal of Critical Reviews*, 7(1), 414-420.

Rani, D., & Ranjan, R. K. (2014). A comparative study of SaaS, PaaS and IaaS in cloud computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(6).

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.

Schulze, H. (2020). *Cloud Security Report.* Cybersecurity Insiders. Available at: https://www.isc2.org/Resource-Center/Reports/Cloud-Security-Report/-/media/44A81ED54571463997B1DDACE905665F.ashx .Accessed : 04 may 2021

Shankarwar, M. U., & Pawar, A. V. (2015). Security and privacy in cloud computing: A survey. In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014* (pp. 1-11). Springer, Cham.

Shibli, M. A., Masood, R., Habiba, U., Kanwal, A., Ghazi, Y., & Mumtaz, R. (2014). Access control as a service in cloud: challenges, impact and strategies. In *Continued Rise of the Cloud* (pp. 55-99). Springer, London.

Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Kumar, A. D. (2019, February). A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques. In *Intelligent Communication Technologies and Virtual Mobile Networks* (pp. 252-270). Springer, Cham.

Tadapaneni, N. R. (2020). Cloud Computing Security Challenges. *International Journal of Innovations in Engineering Research and Technology*, 6(7) (pp. 1-6)

Tahboub, R., & Saleh, Y. (2014, January). Data leakage/loss prevention systems (DLP). In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-6). IEEE.

Tirumala, S. S., Sathu, H., & Naidu, V. (2015, December). Analysis and prevention of account hijacking based incidents in cloud environment. In *2015 international Conference on Information Technology (ICIT)* (pp. 124-129). IEEE.

Ujjwal, K. C., Garg, S., Hilton, J., Aryal, J., & Forbes-Smith, N. (2019). Cloud Computing in natural hazard modeling systems: Current research trends and future directions. *International Journal of Disaster Risk Reduction*, *38*, 101188.

Usman, A., Awwalu, J., & Kamil, B. (2016). Security threat on Cloud Computing. *International Journal of Emerging Trends & Technology in Computer Science* (pp. 18-21)

Watson, M. R., Marnerides, A. K., Mauthe, A., & Hutchison, D. (2015). Malware detection in cloud computing infrastructures. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 192-205.

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, 7(1), 1-12.

Zafar, F., Khan, A., Malik, S. U. R., Ahmed, M., Anjum, A., Khan, M. I., & Jamil, F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Computers & Security*, *65*, 29-49.