Tommi Törmänen

INFORMATION SECURITY AND RISK MANAGEMENT OF CLOUD SERVICES: GUIDELINES AND RECOMMENDATIONS FOR ORGANIZATIONS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

ABSTRACT

Törmänen, Tommi
Information Security and Risk Management of Cloud Services: Guidelines and Recommendations for Organizations.
Jyväskylä: University of Jyväskylä, 2024, 86 pp.
Cyber Security, Master's Thesis
Supervisor(s): Viinikainen, Ari

Cloud solutions have been the standard IT platform for over a decade and are increasingly adopted by organizations and consumers. Despite the strong trend of users and organizations moving to cloud solutions, cloud security remains a significant issue and a longstanding debate among both academics and practitioners, and many organizations are still hesitant to adopt cloud solutions due to security concerns. The objective for this thesis was to improve awareness among organizations regarding the security risks associated with cloud computing and the methods and tools available to mitigate these risks. The study aimed to answer one main research question: *"What should organizations take into account regarding information security when deploying and managing cloud services?"*, and one sub-research question: *"What information security risks can the use of cloud services cause for organizations?"*. The structure of the thesis encompasses a thorough literature review, followed by an empirical case study. The numerous challenges associated with cloud security highlight the critical need for organizations to implement robust security controls, conduct comprehensive risk assessments, and ensure continuous monitoring and development of their cloud environments. It is essential for organizations to remain adaptive and commit to continuous improvement to ensure that cloud security evolves alongside the cloud environment and the surrounding threat landscape. Organizations should adopt a comprehensive and multilayered approach to cloud security, adhering to the defense-in-depth principles. This includes ensuring that security is integrated into every layer of the cloud architecture by design.

Keywords: cloud computing, cloud services, information security, risk management

TIIVISTELMÄ

Törmänen, Tommi
Pilvipalveluiden tietoturva ja riskienhallinta: Ohjeet ja suositukset organisaatioille
Jyväskylä: Jyväskylän yliopisto, 2024, 86 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Viinikainen, Ari

Pilviratkaisut ovat olleet standardi IT-alusta yli vuosikymmenen ajan, ja organisaatiot sekä kuluttajat ottavat niitä käyttöön yhä enenevissä määrin. Huolimatta kuluttajien ja organisaatioiden vahvasta suuntauksesta siirtyä pilviratkaisuihin, pilven tietoturva on edelleen merkittävä ongelma ja pitkäaikainen keskustelunaihe sekä tutkijoiden että ammattilaisten keskuudessa. Monet organisaatiot epäröivät edelleen ottaa pilviratkaisuja käyttöön tietoturvaongelmien vuoksi. Tämän pro gradu -tutkielman tavoitteena oli lisätä organisaatioiden tietoisuutta pilvipalveluihin liittyvistä tietoturvariskeistä sekä käytettävissä olevista menetelmistä ja työkaluista näiden riskien hallitsemiseksi. Tutkimuksen tavoitteena oli vastata yhteen päätutkimuskysymykseen: "*Mitä organisaatioiden tulisi ottaa huomioon tietoturvan osalta pilvipalveluiden käyttöönotossa ja hallinnassa?”*, sekä yhteen apututkimuskysymykseen: "*Mitä tietoturvariskejä pilvipalveluiden käyttö voi aiheuttaa organisaatioille?*". Opinnäytetyön rakenne käsittää perusteellisen kirjallisuuskatsauksen, jota seuraa empiirinen tapaustutkimus. Pilven tietoturvaan liittyvät lukuisat haasteet korostavat organisaatioiden kriittistä tarvetta toteuttaa vaikuttavia tietoturvakontrolleja, suorittaa kattavia riskinarviointeja, ja varmistaa pilviympäristöjensä jatkuva valvonta sekä kehitystyö. Organisaatioiden on tärkeää pysyä mukautuvina ja sitoutua jatkuvaan parantamiseen varmistaakseen, että pilven tietoturva kehittyy pilviympäristön ja ympäröivän uhkaympäristön mukana. Organisaatioiden tulisi omaksua kattava ja monitasoinen lähestymistapa pilven tietoturvaan noudattaen syvyyssuuntaisen suojauksen periaatteita. Tähän sisältyy sen varmistaminen, että tietoturva on integroitu pilviarkkitehtuurin jokaiseen kerrokseen suunnitellusti.

Asiasanat: pilvilaskenta, pilvipalvelut, tietoturvallisuus, riskienhallinta

FIGURES

TABLES

TABLE OF CONTENT

1 INTRODUCTION

Most of us use cloud services on a daily basis without realizing it or giving it a second thought, such as services like Microsoft 365, Gmail, and iCloud (Chauhan & Shiaeles, 2023). Given that Amazon Web Services, Google Cloud, and Microsoft Azure are considered the most popular cloud service providers, it is likely more challenging to find an organization that does not utilize some of their services to some extinct than one that does (Qazi, 2023). Indeed, cloud solutions have been the standard IT platform for over a decade and are increasingly adopted by organizations and consumers, with more workloads continuously migrating from traditional storage to the cloud. (Gururaj et al., 2017: Mandal & Khan, 2021).

Cloud computing fundamentally relies on virtualization and distributed computing technology, integrating IT resources such as computing power, storage, and networking into high-performance services that customers can access over networks, paying only for what they use on an on-demand basis (Khan & Al-Yasiri, 2016; Mandal & Khan, 2021; Xiaojun & Qiaoyan, 2010). The success of cloud computing is driven by a combination of market and technology factors (Coppolino et al., 2017; Rebollo et al., 2015). Organizations operate in a constantly evolving environment and must quickly adapt their IT operations to keep pace (Coppolino et al., 2017; Mandal & Khan, 2021). The number of services and applications being deployed and decommissioned is continuously rising, and the availability of cheaper processors, lower latency networks, and advancements in virtualization technologies are encouraging organizations to shift their operations from local IT platforms to distributed cloud environments (Coppolino et al., 2017; Rebollo et al., 2015).

Especially for small and medium businesses, cloud solutions provide a cost-effective and low barrier access to industry best practice tools and resources fast, which would otherwise be out of their reach (Morsy et al., 2016: Subashini & Kavitha, 2010). In addition to cost-efficiency, cloud solutions offer organizations multiple other attractive benefits, such as operational efficiency and the ability to quickly acquire or dispose of resources like storage and

memory (Avram, 2014; Beckers et al., 2013; Chang et al., 2016; Mandal & Khan, 2021; Somorovsky et al., 2011).

Despite the strong trend of users and organizations moving to cloud solutions, cloud security remains a significant issue and a longstanding debate among both academics and practitioners (Singh & Chatterjee, 2017; Subramanian & Tamilselvan, 2019; Xiaojun & Qiaoyan, 2010). Cloud security ranks among the top priorities for organizations because if the security level is inadequate, the cloud services and resources may not be reliable, compromising the security of data, applications, and infrastructure stored in the cloud (Alassafi et al., 2017; Chang et al., 2016; Chauhan & Shiaeles, 2023; Mandal & Khan, 2021). Simultaneously, academics consider cloud security an important research topic due to its complexity and significant impact on numerous stakeholders (Singh et al., 2016; Somorovsky et al., 2011).

The appeal of cloud solutions as targets for criminals and other malicious groups is evident, given that organizations and consumers are increasingly migrating valuable data and services to the cloud (Mandal & Khan, 2021; Subashini & Kavitha, 2010).This is just one of the reasons for the phenomenon where despite the fact that cloud solutions have been widely in use for over a decade, many organizations are still hesitant to adopt cloud solutions due to security concerns (Arora et al., 2017; Beckers et al., 2013; Sun, 2018; Xiaojun & Qiaoyan, 2010; Zissis & Lekkas, 2012).

In the midst of the flood of information and offers related to cloud security solutions, it can be difficult for organizations to understand what should be treated as essential, which information security controls should they focus on, and which guidelines or frameworks to rely on (Kalaiprasath et al., 2017). From an organizational perspective, the problem can be considered to be multidimensional, and among other things, it is concretized in the form of shortage of talent, lack of maturity, conflicting best practices and frameworks, and complex commercial structures of the service providers and suppliers (Gururaj et al., 2017; Zhu et al., 2012). The complexity is heightened because, despite cloud solutions sharing many fundamental components and technologies with traditional IT systems, traditional security mechanisms and controls may prove to be ineffective and inefficient with cloud environments (Khalil et al., 2014; Zissis & Lekkas, 2012).

Coppolino et al. (2017) suggest that for cloud solutions to be considered a viable alternative, their security level should match or exceed that of traditional IT systems. Achieving this requires raising awareness about the security issues associated with cloud computing and the methods and tools available to mitigate these risks (Coppolino et al., 2017). This thesis aims to assist organizations on this objective by examining the security risks in cloud computing and identifying how and why these risks should be addressed when adopting or using cloud services.

The scope of the study is primarily limited to organizations operating in the private sector, although the findings can also be applicable to public sector organizations to a certain extent. Industry-specific regulations and mandatory standards are excluded from the scope of the study. When examining specific cloud platforms and their technical features, the scope is limited to the largest and most widely used platforms, namely Amazon Web Services, Google Cloud Platform, and Microsoft Azure (Wright et al., 2023).

Since English is not the author's native language, the artificial intelligence (AI) based text editor ChatGPT was used to improve the readability of the thesis and to ensure grammatical correctness (OpenAI, 2024). However, ChatGPT or other AI-based tools were not used for any other purposes, such as serving as a scientific source or generating content from scratch. The use of ChatGPT during the thesis work was strictly limited to rephrasing sentences the author had first produced himself or written based on academic articles and other scientific sources. The sentences rephrased by ChatGPT were then carefully reviewed by the author to ensure that the content was not distorted, and they were factually correct. The rephrased sentences were mostly used as they were or modified by the author if deemed necessary.

The structure of the thesis is organized as follows: the second and the third chapter form the literature review section of the thesis. The second chapter first introduces the definition of cloud computing and cloud services, describes the actors involved, and explores the service delivery and deployment models used in cloud computing. Towards the end of the second chapter, it identifies and explains the basic elements of cloud architecture, followed by a concise overview of the advantages organizations can gain through the adoption of cloud solutions. The third chapter describes the typical risks associated with cloud security from the organizations' perspective and describes potential security measures than can be employed to mitigate these risks. The empirical section of the thesis begins from the fourth chapter, focusing on the research methods used in the study, their implementation, and the process of data collection using a survey. The fifth chapter presents the survey results and their analysis. Finally, the study's findings are discussed in the sixth chapter, followed by a conclusion of the thesis in the seventh chapter.

2 CLOUD COMPUTING

In the early 90s computers with high performance capabilities were connected with each other using fast data transfer techniques to facilitate complex computations and data-heavy scientific tasks (Stanoevska-Slabeva et al., 2010; Zissis & Lekkas, 2012). The early predecessor of cloud computing called grid computing was introduced to the public, and the story of cloud computing had begun (Kandukuri et al., 2009; Zissis & Lekkas, 2012). The term "cloud computing" itself derives from the cloud symbol frequently employed to represent the internet in diagrams and flowcharts (Butt et al., 2022; Zissis & Lekkas, 2012) and gained prominence following Amazon's introduction of Amazon Web Services in 2006 (Walterbusch ym., 2017).

Cloud computing is considered as the next generation of revolutionary internet-based distributed computing systems enabling remote access to high-performance computing resources and services without the need to invest in physical infrastructure (Chauhan & Shiaeles, 2023; Morsy et al., 2016; Rao & Selvamani, 2015). It offers users convenient and customizable access to a range of applications and utilizes virtualization to efficiently allocate resources providing flexibility, scalability, and cost-effective IT resource management (Chauhan & Shiaeles, 2023; Rao & Selvamani, 2015; Singh et al., 2016).

Khalil et al. (2014) equated cloud computing to utility-based systems like water, sewage and electricity as cloud computing offers a centralized pool of configurable computing resources and outsourcing mechanisms, facilitating the delivery of various computing services to diverse users. They used electricity as an example analogy, as people are nowadays connected to centralized electricity grids, backed by power utilities instead of depending on their own electricity generation capabilities (Khalil ym., 2014). Numerous organizations have progressively recognized the advantages of migrating their applications and data to the cloud when comparing to purchasing and maintaining infrastructure of their own (Deyan & Hong, 2012).

2.1 Definition

Cloud computing has been extensively in the scope of the research community for many years and various definitions of cloud computing have been introduced. Soms et al. (2022) defined cloud computing as "*an on-demand delivery of IT resources over the internet with pay-as-you-use pricing*". According to Subramanian & Tamilselvan (2019) cloud computing can be defined as "*form of distributed computing paradigm that involves using the Internet to deliver a host of services*". However, the most widely accepted definition of cloud computing is introduced by the National Institute of Standards and Technology (NIST) (Deyan & Hong, Jansen, 2011; Morsy et al., 2016; Singh & Chatterjee, 2017; Walterbusch ym., 2017) which is also going to be referred to in this paper:

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011).

In the NIST definition Mell & Grance (2011) also describe the five main characteristics of cloud computing which are:

- **On-demand self-service.** Users are able to access and use the cloud computing resources and services independently without human interaction.

- **Broad network access.** The data and services in the cloud are available to be accessed over the network with standard protocols and devices.

- **Resource pooling.** The computing resources, physical and/ or virtual, provided by the cloud provider serve multiple users and are allocated in dynamic way using a multi-tenant model.

- **Rapid elasticity.** The used cloud computing resources can be elastically scaled accordingly with the customer's needs in an on-demand way.

- **Measured service.** The cloud system automatically monitors and measures the customer's resource usage and needs while automatically scaling and optimizing the provided resources.

2.2 Actors

The NIST Cloud Computing Reference Architecture by Liu et al. (2011) recognizes five key actors who have a distinct and specialized role in cloud computing activities (Bohn ym., 2011; Gururaj ym., 2017):

- **Cloud consumer** is a person or an organization who purchases and/ or utilizes the IT resources or services either from a Cloud Service Provider or a Cloud broker (Bohn ym., 2011; Butt et al., 2022; Liu et al., 2011; Singh & Chatterjee, 2017).

- **Cloud provider,** also known as Cloud Service Provider (CSP). CSP can be an organization or an individual who is responsible for the overall management of the cloud (Bohn ym., 2011). This includes establishing and maintaining the cloud computing infrastructure, running the cloud software providing the services, and making the cloud infrastructure and services available to cloud consumers via network access (Butt ym., 2022; Liu et al., 2011; Morsy ym., 2016).

- **Cloud auditor** is an entity (usually a third-party) who can be used to examine and evaluate the services and CSPs cloud service controls. This can be necessary for example to ensure that security, privacy, and performance have been appropriately implemented and compliant with relevant standards or regulations for example (Bohn ym., 2011; Liu et al., 2011; Singh & Chatterjee, 2017).

- **Cloud broker** can help the cloud consumers by helping them to acquire and/ or manage their cloud services, as this can turn out to be a too complex task for many of the cloud consumers to take care own their own (Bohn ym., 2011; Butt ym., 2022; Liu et al., 2011).

- **Cloud carrier** is the intermediary between the CSPs and cloud consumers, who provides the connections and access to consumers through network and telecommunication devices such as computers and mobile devices (Bohn ym., 2011; Liu et al., 2011).

2.3 Service Delivery and Deployment Models

Amongst practitioners and the research community, three different major service delivery models and four deployment models are widely referenced (Beckers et al., 2013; Deyan & Hong, 2012; Jansen, 2011; Morsy et al., 2016; Rao & Selvamani, 2015; Rizvi et al., 2017; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010), and also recognized by the NIST definition of cloud computing

(Mell & Grance, 2011). Cloud computing offers flexible resource utilization and specialization, and each service delivery model may also coexist within a single cloud platform and offer different possible implementations (Jansen, 2011; Morsy et al., 2016). The three available service delivery models in cloud computing are:

- **Software as a Service (SaaS)** enables cloud customers to utilize one or more applications offered by the CSP, which are running on cloud infrastructure via the internet as an on-demand service (Beckers et al., 2013; Jansen, 2011; Morsy et al., 2016; Rizvi et al., 2017; Singh et al., 2016). Customers can remotely access the applications from various client devices without requiring installation of the applications to their devices, via either a thin client interface, such as a web browser, or a program interface (Mell & Grance, 2011; Morsy et al., 2016; Singh et al., 2016; Subashini & Kavitha, 2010). The customers do not manage or control the underlying cloud infrastructure or individual application functionalities, except for potentially limited user-specific application settings (Mell & Grance, 2011; Subashini & Kavitha, 2010).

- **Platform as a Service (PaaS)** provides a programmable computing platform as an on-demand service in which cloud customers can create, deploy, execute and manage their own applications, leveraging programming languages, developing tools and other tools supported by the CSP without requiring installation of the platforms or supported tools on their local devices (Beckers et al., 2013; Jansen, 2011; Morsy et al., 2016; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010). The customers can control the applications but cannot manage or control the underlying cloud infrastructure, like network, servers, operating systems or storage, with the exception that they may have some control over the configurations of the application-hosting environment (Mell & Grance, 2011; Singh et al., 2016; Subashini & Kavitha, 2010).

- **Infrastructure as a Service (IaaS)** model is based on virtualization technology and is the most closely aligned with physical resources, providing basic computing infrastructure like storage and computation resources (e.g., virtual machines) and network for the cloud customers to utilize as an on-demand service (Beckers et al., 2013; Jansen, 2011; Morsy et al., 2016; Rizvi et al., 2017; Singh & Chatterjee, 2017). The customer cannot manage or control the underlying cloud infrastructure but is able to install and operate arbitrary software and might also have some control over selected network components (Mell & Grance, 2011; Rao & Selvamani, 2015; Subashini & Kavitha, 2010).

For deployment models, cloud computing presents different solutions. Private cloud, public cloud and hybrid cloud are widely recognized as the major deployment models by the research community (Beckers et al., 2013; Butt et al., 2022; Morsy et al., 2016), but many also include a fourth deployment to the list called community cloud (Mell & Grance, 2011; Singh & Chatterjee, 2017; Singh et al., 2016; Subashini & Kavitha, 2010). The following deployment models have been identified for cloud solutions in this paper:

- **Private cloud.** The cloud infrastructure is dedicated to a specific organization, and it is operated and managed by the organization itself or a third party (Beckers et al., 2013; Morsy et al., 2016; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010). The cloud infrastructure can be on-premises or off-premises and it is owned by the organization itself and implemented within the organization's computing environment (Jansen, 2011; Singh et al., 2016; Subashini & Kavitha, 2010).

- **Community cloud.** The cloud infrastructure is deployed and shared among a group of people or organizations and is designed to meet the specific needs of a particular community (Singh & Chatterjee, 2017; Subashini & Kavitha, 2010). The management of community cloud can be done by one or more of the organizations or by a third party, and it can be hosted either on-premises or off-premises (Mell & Grance, 2011; Subashini & Kavitha, 2010).

- **Public cloud.** The cloud infrastructure is made available to open use of the public or a broad industry sector (Beckers et al., 2013; Mell & Grance, 2011; Morsy et al., 2016; Subashini & Kavitha, 2010). The cloud infrastructure is owned, managed, and operated by the cloud service provider and multiple users share the cloud resources (Mell & Grance, 2011; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010).

- **Hybrid cloud.** The cloud infrastructure is a combination of two or more different cloud deployment models that remain separate entities but are interconnected, e.g., a private cloud which is capable of using public cloud resources (Morsy et al., 2016; Subashini & Kavitha, 2010).

2.4 Cloud Architecture

Cloud solutions can be considered as very complex systems with significant amount of hardware and software components (Beckers et al., 2013; Gururaj et al., 2017). Cloud computing is based on virtualization technology, which according to Zissis & Lekkas (2012) was introduced already in 1967, but for a long time was only used in main frame systems. In general, virtualization means that a host computer runs a hypervisor application, which generates one or more virtual machines capable of accurately simulating real computers and executing any software, ranging from operating systems to end-user applications (Naone, 2009). The cloud computing model relies on a layered stack of dependent objects such as virtual machines, application programming interfaces, servers, and applications, where the users and the applications used are located on the top layer of the stack, and the physical infrastructure and servers on the lower layer, while the higher layers are dependent upon the lower layers (Morsy et al., 2016; Singh et al., 2016).

The IaaS model covers the cloud's physical infrastructure layer, the virtualization layer, and the layer of virtualized resources, and abstracts them into a collective pool of computing resources (Morsy et al., 2016; Singh et al., 2016). The infrastructure layer oversees the computing capabilities such as performance, bandwidth, and storage access (Singh et al., 2016). The cloud environment offers various storage models such as shared file/ block storage system, object storage system, and database or table storage system, each solution with its own advantages and limitations (Singh & Chatterjee, 2017). In the physical layer, various hardware components such as processors, hard drives, and network devices are located in data centers, which are geographically independent locations responsible for fulfilling storage and processing requirements (Zissis & Lekkas, 2012). Data centers contain both physical and virtualized IT resources, integrating multiple technologies and components that are usually interconnected (Singh & Chatterjee, 2017).

Virtualization is considered to be a critical component for the cloud, and it enables the essential characteristics of the cloud such as location independence, resource pooling and rapid elasticity (Singh et al., 2016; Zissis & Lekkas, 2012). With virtualization, services, applications, computing resources, and operating systems can be extracted from the hardware on which they run (Singh & Chatterjee, 2017). Virtualization could be simply described as converting physical IT resources into virtual versions, such as servers, storage and network (Microsoft, 2024b; Singh & Chatterjee, 2017). Its main components are the Virtual Machine (VM) and the Virtual Machine Manager (VMM), often referred also as the hypervisor (Broadcom, 2024a; Singh & Chatterjee, 2017).

A VM can be thought as virtual computer that utilizes software instead of a physical computer to execute programs and deploy apps (Broadcom, 2024b; Microsoft, 2024). One or more VMs can operate on a physical "host" machine,

with each VM running its own operating system and applications, functioning independently of the other VMs (Amazon Web Services, 2024b; Broadcom, 2024b). VMs are stored to the host machine as image files, which can be easily moved to another device, copied or cloned (Singh & Chatterjee, 2017). VMs can be accessed with a software called a hypervisor, which enables one physical host computer to run multiple VMs by virtually allocating the underlying hardware resources to individual VMs as required and connecting multiple VMs with each other if needed (Amazon Web Services, 2024b; Broadcom, 2024a; Singh & Chatterjee, 2017). This can be used to facilitate multi-tenancy, which allows multiple customers or users from the same or different organizations to share resources and applications without visibility or access to each other's data (Singh et al., 2016). Multi-tenant applications make it possible for each tenant to individually manage various features of the application, such as user interface and access control (Singh & Chatterjee, 2017).

The PaaS model covers the platform layers, APIs, and service layers. PaaS layer is dependent on the virtualization of resources provided by the IaaS layer (Morsy et al., 2016). The increasing use of mobile devices and the popularity of APIs are one of the key reasons for the exponential growth of cloud computing services and more and more organizations migrating their data to the cloud (Qazi, 2023). An API serves as a software interface enabling digital devices, software applications, and data servers to communicate and interact with each other, and today the majority leading cloud platforms utilize APIs to manage all their user-related operations, such as identity management (Qazi, 2023). Cloud APIs enable the development of cloud infrastructure, software, services, and applications for many cloud platforms, and can be provided as an IaaS API to support the provision of computing and storage, SaaS API to connect to software or applications, or PaaS API to create applications and software. APIs rely on set protocols such as Simple object access control (SOAP) and representation state transfer (REST) which define how applications or databases can establish connections and communicate with each other. SOAP API protocol is more commonly used by security critical organizations as it is considered more secure than REST API protocol, which lacks the inherent security features and extensions found in SOAP, thus relying on the APIs themselves when it comes to security. GraphQL is a newer query language API standard introduced by Facebook that serves as an alternative to REST API and has some additional features compared REST, such as security measures, but is considered to be slow when executing large or complicated queries and prone to complex security implications. (Qazi, 2023)

On the top of the layer stack, the SaaS model includes the applications and services provided to the end users. SaaS layer relies on the PaaS layer to host the services and IaaS layer to optimize resource utilization for multi-tenant delivery (Morsy et al., 2016). The application level is located at the topmost level, directly delivering the software to the users through an interface without the

need to install the software to client devices (Singh et al., 2016). The applications themselves are developed using the programming interfaces of the services located on the PaaS layer, which are accessible through the internet and often involve multiple intercommunicating cloud components (Jansen, 2011).

An additional layer called the middleware layer resides between the application layer and the underlying platform, providing services from database servers to the software applications (Singh et al., 2016). Singh et al. (2016) characterize middleware as the glue software program that simplifies the implementation of communication for software developers within a cloud environment, and it is considered to be one of the standard technologies used to build cloud environments (Singh & Chatterjee, 2017).

2.5 Advantages

Cloud computing can offer significant benefits for both individuals and organizations (Khalil et al., 2014). The growing complexity of managing software and IT infrastructure results in computing becoming increasingly more expensive for organizations, especially small and medium-sized ones (Esposito & Castiglione, 2016). Cloud solutions give organizations the opportunity to outsource their IT infrastructures to a CSP, by utilizing cost-effective, scalable, and location-independent platforms (Rizvi et al., 2017). This enables organizations to decrease their IT costs which is usually the main goal for organizations planning on migrating to the cloud, while it simultaneously eases the burden from managing and maintaining their own in-house IT infrastructure (Alassafi et al., 2017; Esposito & Castiglione, 2016; Rizvi et al., 2017).

The basic business principle for cloud computing adheres to a simple pay-for-use pricing model, offering customers the ability to reduce their expenditure by provisioning a specific amount of resources, which are provided to the customer as on-demand service (Singh et al., 2016). This way cloud computing can also reduce the barrier to entry for smaller firms and presents a considerable opportunity for many developing countries that have lacked the resources and have not been fully able to participate in the IT revolution before (Avram, 2014). Avram (2014) emphasizes that cloud computing can also reduce IT barriers to innovation and enables the emergence of novel applications and services. Cloud solutions can provide nearly instant access to hardware resources with reduced capital investments, and this way also accelerating deployment and time to market for businesses (Avram, 2014; Esposito & Castiglione, 2016).

Rapid elasticity is considered as one of the main characteristics of cloud computing (Mell & Grance, 2011), and it means that resources and services can be quickly scaled up and down for customers and users (Avram, 2014; Beckers et al., 2013). The cloud combines resources such as storage, processing, memory,

virtual machines, and network bandwidth into a unified pool, and can dynamically allocate and reallocate them according to the customers' needs and use, while similarly optimizing utilization of existing resources of the CSP (Beckers et al., 2013; Esposito & Castiglione, 2016; Zissis & Lekkas, 2012).

Cloud solutions usually feature advanced security technologies and controls that can be implemented throughout the cloud, mostly available as a result due to data centralization and universal architecture (Alassafi et al., 2017; Zissis & Lekkas, 2012). Together with the automation capabilities and CSPs typically more extensive security resources, this often results in more advanced security capabilities than could be achieved with traditional in-house IT structures and models, managed by a group of people with various other responsibilities (Butt et al., 2022; Khalil et al., 2014; Mandal & Khan, 2021; Zissis & Lekkas, 2012).

3 CLOUD SECURITY AND RISKS

While there are numerous unique advantages to adopting cloud solutions, there are also unique challenges which cannot be ignored, with security being one of the key concerns (Avram, 2014; Coppolino et al., 2017; Esposito & Castiglione, 2016; Singh et al., 2016; Soms et al., 2022). Cloud security still poses a major concern for organizations, and many remain hesitant to adopt cloud solutions fearing that their sensitive information or critical services could be compromised (Morsy et al., 2016; Singh et al., 2016; Subramanian & Tamilselvan, 2019). This highlights the importance of cloud security and the necessity to enhance security in the cloud environment to speed up the adoption of cloud services and to address regulatory requirements (Esposito & Castiglione, 2016; Subashini & Kavitha, 2010; Subramanian & Tamilselvan, 2019).

The amount of security attacks targeting cloud solutions continues to rise as the cloud has become an increasingly appealing target for attackers due to its high adoption rate and the valuable resources stored in and supported by the cloud (Mandal & Khan, 2021; Khalil et al., 2014; Singh et al., 2016). Especially the upper layers of the cloud, for which cloud customers are responsible, have become more susceptible to attacks, primarily due misconfigurations and human errors (Torkura et al., 2021). The potential of cloud computing has not gone unnoticed from the attackers either and the attackers are leveraging the cloud infrastructure as well to carry out attacks (Duncan, 2020; Singh & Chatterjee, 2017). Jansen (2011) equated data to the currency of 21st century and cloud environments to the banks where the currency is kept. Similarly to traditional banks became attractive targets for robbers, the cloud environments are also attractive to the modern-day cyber criminals and other threat agents. The attack vectors associated with cloud computing are similar to those threatening traditional network and computer security (Sun, 2018), and are mainly focusing either on network, hypervisor, or hardware layers (Coppolino et al., 2017). The attackers, also known as threat agents, may consist of internal users, external parties, and even the CSP itself can function as a threat agent (Coppolino et al., 2017; Singh & Chatterjee, 2017). External threat agents primarily execute attacks over networks, whereas internal threat agents, also

referred as malicious insiders, have the capability to launch attacks from within the cloud infrastructure, functioning as internal users or employees of the CSP, for example (Coppolino et al., 2017).

In information security, it is crucial to understand the requirements and specific security needs in order to be able to design sufficient security solutions (Zissis & Lekkas, 2012). However, in the distributed environment of the cloud, with multiple users possessing diverse security requirements and needs, which the CSP is not always aware of, the cloud presents a unique security challenge and demands considerable expenses and resources from the CSPs (Almorsy et al., 2011; Arora et al., 2017; Morsy et al., 2016; Zissis & Lekkas, 2012). From the cloud customers perspective lack of visibility and transparency can also lead to security issues. Due to transparency issues in a multi-tenant environment, many CSPs do not permit customers to implement their own security monitoring or intrusion detection systems into the IaaS layer (Singh & Chatterjee, 2017).

The complexity of the cloud infrastructure, comprised of technology, processes, personnel, and commercial constructs, generates a vast landscape of potential vulnerabilities and requires a holistic security strategy (Duncan, 2020; Gururaj et al., 2017; Singh & Chatterjee, 2017; Somorovsky et al., 2011). Each cloud computing service delivery model has different level of security requirements, and just as capabilities are inherited between them, so are the information security issues and risks (Morsy et al., 2016; Subashini & Kavitha, 2010). Past research has extensively researched and documented the risks and vulnerabilities related to cloud computing, and each CSP and customer must implement countermeasures and security controls to mitigate the risks according to their assessment (Gururaj et al., 2017; Singh & Chatterjee, 2017). The primary purpose of security controls is to maintain security in the cloud infrastructure (Soms et al., 2022). Organizations should first fully understand their users' activities in the cloud and identify potential attack surfaces and weaknesses before assessing which native and third-party controls will be the most effective on preventing and responding to threats identified (Duncan, 2020; Singh & Chatterjee, 2017).

Elasticity and multi-tenancy are one of the cloud's key characteristics, but both have significant implications for the security of the cloud (Morsy et al., 2016; Singh et al., 2016; Subramanian & Tamilselvan, 2019). The cloud utilizes virtualization to achieve multi-tenancy, but VMs and hypervisors, like any other software, contain vulnerabilities posing a direct threat to the security and privacy of cloud services (Singh & Chatterjee, 2017). However, CSPs have enhanced the security of the IaaS layer over the years to that extent that attacks at this layer are now less common (Torkura et al., 2021). The nature of the cloud still inherently promotes information sharing, which in turn heightens the risk of unauthorized access to other users' content and information (Subramanian & Tamilselvan, 2019).

Interoperability between cloud platforms also remains a challenge, as many CSPs have not yet developed seamless compatibility (Rizvi et al., 2017). This complicates data and application migration between different platforms and providers, heightening the risk of vendor lock-in for organizations (Rizvi et al., 2017; Singh & Chatterjee, 2017). Lack of interoperability can also prevent organizations from deploying different cloud platforms for different applications and tools, or result in organizations being unable to deploy for example their existing security and identity management policies and tools for applications running on different cloud platforms (Avram, 2014; Rizvi et al., 2017). Portability is another cloud specific issue worth to mention, and it refers to the ability to transfer data and applications among CSPs with as minimal integration challenges as possible (Rizvi et al., 2017). Organizations are increasingly dependent on cloud solutions for their daily operations, storing significant amounts of data in the cloud (Rizvi et al., 2017). There are number of reasons why the organizations might find themselves looking into migrating their data to another cloud platform, making portability a critical enabler for wide adoption of cloud computing, which organizations need to carefully consider when selecting a CSP (Avram, 2014; Rizvi et al., 2017).

In addition to cloud specific threats, Butt et al. (2022) identifies traditional information and network related threats as major risks of cloud computing. Consequently, the security controls used to protect the cloud are somewhat similar to those used in traditional IT, but do not necessarily fully address the risks affiliated with cloud computing (Deyan & Hong, 2012; Khan & Al-Yasiri, 2016). The basic principles of information security also apply in cloud security, with the objective being to protect of the confidentiality, integrity, and availability of cloud assets (Butt et al., 2022; Chauhan & Shiaeles, 2023; Deyan & Hong, 2012; Rao & Selvamani, 2015; Singh & Chatterjee, 2017; Zissis & Lekkas, 2012).

3.1 Confidentiality, Integrity, and Availability

In cloud computing it's common for users of the cloud solutions to share and store their information on remote servers owned and operated by third parties and accessed via the internet or other networks. The material stored and shared in the cloud can be anything from sensitive personal identifying information (PII) to operation critical business information and governmental information. The risks naturally vary depending on the cloud customer and the information, but it is obvious that when individuals or organizations handle or store information in the cloud, concerns about confidentiality are usually present as well. (Rao & Selvamani, 2015; Subashini & Kavitha, 2010).

Confidentiality means that the information assets can only be accessed by authorized parties or systems, often associated with authentication in the cloud context (Singh & Chatterjee, 2017; Zissis & Lekkas, 2012). The complex nature of

the cloud and various parties, devices, and applications being involved, leads to an increased amount of access points and an expanded attack surface, therefore also increasing the risk of the data being compromised (Singh & Chatterjee, 2017; Zissis & Lekkas, 2012). Software confidentiality is another term related to cloud security, indicating trust in specific applications or processes to manage and handle data securely (Zissis & Lekkas, 2012). For instance, the elasticity of cloud environments could potentially result to software confidentiality issues, as the scaling of a tenant's resources may provide other tenants with the opportunity to utilize resources that were previously allocated to another tenant (Morsy et al., 2016).

Integrity is considered as one of the key elements of information security, and insufficient integrity controls can lead to serious issues regardless of the system in question (Subashini & Kavitha, 2010; Zissis & Lekkas, 2012). Integrity refers to that information assets can only be modified by authorized parties, while data integrity aims to ensure the protection of data against unauthorized deletion, modification, or fabrication, which all can be done intentionally or by accident (Singh & Chatterjee, 2017; Zissis & Lekkas, 2012). Achieving data integrity is much easier in standalone systems having a single database, when comparing to a distributed systems with multiple databases such as the cloud environment (Subashini & Kavitha, 2010). Ensuring data integrity in a cloud setting requires preventing unauthorized access to data and managing transactions across multiple data sources in a fail-safe manner, as well as automated controls that check and verify that the integrity of data remains uncompromised (Butt et al., 2022; Subashini & Kavitha, 2010; Zissis & Lekkas, 2012).

Availability means that the IT resources can be accessed and used by authorized entities, even in the case of possible security events and incidents such as errors or breaches, and the system will operate as needed when needed (Gururaj et al., 2017; Jansen, 2011; Singh & Chatterjee, 2017; Zissis & Lekkas, 2012). When people are talking about availability they usually refer primarily to software and data, but it applies to network and hardware infrastructure as well (Singh ym., 2016; Zissis & Lekkas, 2012). A single hardware failure could potentially affect the availability of the whole system (Singh & Chatterjee, 2017). CSPs need to ensure that cloud services are available 24/7 as the daily operations of many organizations depend on cloud services, thus making high availability level of the services crucial (Avram, 2014; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010; Xiaojun & Qiaoyan, 2010; Zissis & Lekkas, 2012). This requires an infrastructure that supports load-balancing, resiliency to hardware and software failures, and also against malicious influencing such as denial of service attacks (Singh et al., 2016; Subashini & Kavitha, 2010).

The risk of permanent or accidental loss of data stored in the cloud is known as the data loss threat, which is an important concern for cloud security (Butt et al., 2022; Chauhan & Shiaeles, 2023). Despite the numerous data

redundancy and backup systems offered by the cloud, there are still circumstances that can lead to data loss (Chauhan & Shiaeles, 2023). Examples of factors leading to data loss include intentional and unintentional data deletion or alteration without a backup of the original content, loss of encoding key for encrypted data, and hardware failure (Butt et al., 2022; Kalaiprasath et al., 2017; Singh & Chatterjee, 2017). Any unplanned incidents and emergencies need to be addressed with robust business continuity and disaster recovery plans to ensure that the data is not compromised, and possible downtime and disruptions to business remain as low as possible (Avram, 2014; Chauhan & Shiaeles, 2023; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010; Zhu et al., 2012). Organizations should assess and take into consideration the reliability of the cloud services utilized when designing and implementing business continuity and disaster recovery plans (Jansen, 2011). For mission-critical operations and services dependent on cloud services, besides multi-location data replication processes organizations should consider alternative services, equipment, and locations as backup options in the event of prolonged or permanent outages (Chauhan & Shiaeles, 2023; Jansen, 2011; Singh et al., 2016). CSPs are usually responsible for taking regular backups of customer data to enable quick recovery in the event of disasters, but also to take care that the backup data is safeguarded at least with same level protection as the original data (Singh & Chatterjee, 2017; Singh et al., 2016; Subashini & Kavitha, 2010).

3.2 Cloud Security Management

Cloud computing involves numerous stakeholders, a deep and complex dependency stack, and a high amount of security controls, making cloud security management a complicated task (Morsy et al., 2016). Security policies form the foundation of cloud security (Chang et al., 2016). They are aligned with the organization's security goals and designed to mitigate risks (Chang et al., 2016; Torkura et al., 2021). Organizations should design their security policies and guidelines based on their risk analysis and use them as a standard when planning and implementing the required security controls (Singh & Chatterjee, 2017; Singh et al., 2016).

The adoption of cloud solutions will most likely impact the organization's IT team (Avram, 2014; Gururaj et al., 2017). The roles and responsibilities may evolve, and new skill sets are likely required to effectively maintain cloud controls and to mitigate cloud related IT risks (Avram, 2014). The IT team may also face unforeseen risks. For instance, developers working in the R&D teams might create new accounts or make changes that suit their needs without security or visibility to the IT team in mind (Soms et al., 2022). This presents a security challenge, as the IT team cannot safeguard things that they are unaware of (Soms et al., 2022). Indeed, shadow IT is another threat which needs to be taken into account, and it refers to the use of IT solutions and tools for

business purposes, that are not provided or approved by the organization's IT department, and often without the IT department's knowledge (Walterbusch et al., 2017).

Shadow IT has been present since the dawn of information technology and emergence of cloud computing adds yet another dimension to its complexity (Walterbusch et al., 2017). The root cause for the emergence of shadow IT is the lack of adequate IT solutions that fulfill the needs of employees, also known as the IT gap (Walterbusch et al., 2017). Typically, employees may utilize cloud services alongside with shadow IT, resulting in a situation where there is no documentation of the cloud services used nor the outsourced data or processes (Walterbusch et al., 2017). The issue can be addressed either by improving the current official systems to bridge the IT gap, replacing the unauthorized cloud solutions with official corporate systems, integrating the unauthorized cloud solutions into the corporate IT governance, or by mitigating the risk through the implementation of adequate security controls and creating a safe environment (Walterbusch et al., 2017).

Roles and responsibilities are another important topic for cloud security. Jansen (2011) states that while reduction of costs may be a primary motivation for many organizations to adopt cloud solutions, reducing responsibility for security should not be one. It is critical that organizations operating in the cloud recognize that responsibility for data integrity and protection cannot never be fully delegated, but cloud security is always a shared responsibility between the CSP and the cloud customer (Duncan, 2020; Soms ym., 2022). The security responsibilities can vary significantly between the CSP and the customer depending on the service model in question, and these responsibilities are not always clear to the cloud customers (Subashini & Kavitha, 2010; Torkura et al., 2021). Shared responsibility model is commonly used by CSPs to clearly define the responsibilities for security and compliance between the CSP and cloud customer (Duncan, 2020; Soms et al., 2022; Torkura et al., 2021). Depending on the CSP and the service provided, the model usually follows a principle that the cloud customer is responsible for the security in the cloud, while the CSP is responsible for the security of the cloud (Amazon Web Services, 2024a).

- **In the IaaS model**, the CSP is usually responsible for the underlying infrastructure such as the datacenter, hardware, storage, and network. The customer is responsible for example the operating systems, network security, applications, access policies, identity and access management, endpoints, and information and data. (Amazon Web Services, 2024a; Google, 2024; Microsoft, 2024a; Sisodia & Khan, 2024; Zhu et al., 2012; Zissis & Lekkas, 2012)

- **In the PaaS model**, the CSP is responsible for the same things as in IaaS, but usually also the operating systems and network management. Application layer processes and identity and access

management can be a shared responsibility depending on the CSP and the service provided. The customer is responsible for access policies, endpoints, as well as information and data. (Amazon Web Services, 2024a; Google, 2024; Microsoft, 2024a; Sisodia & Khan, 2024, Zhu et al., 2012)

- **In the SaaS,** model the CSP is typically responsible for everything else but the access policies, endpoints, and information and data, which all fall under the customer's responsibility. (Amazon Web Services, 2024a; Duncan, 2020; Google, 2024, Microsoft, 2024a; Sisodia & Khan, 2024; Zhu et al., 2012)

To ensure effective security management throughout the information supply chain and service lifecycle and eliminating unrealistic expectations, it is critical for organizations and CSPs to agree and document the necessary security requirements and their implementation, and how the related roles and responsibilities are divided (Duncan, 2020; Khalil et al., 2014; Luna et al., 2015 Singh & Chatterjee, 2017). The basic principle should be that the organization is the one who defines the sufficient service level according to its security policies and current level of security (Duncan, 2020), but many times especially with the leading vendors this principle might turn out difficult to achieve (Singh & Chatterjee, 2017).

The agreement for delivering cloud services during the entire lifecycle of the service is established between the CSP and the cloud customer through a Service Level Agreement (SLA) (Kandukuri et al., 2009; Morsy et al., 2016; Singh & Chatterjee, 2017). Both parties are required to adhere to the SLA, with penalties enforced for non-compliance (Morsy et al., 2016; Singh & Chatterjee, 2017). SLAs generally include terms and conditions and objectives related to performance, reliability, security, and agreed monitoring and auditing models (Morsy et al., 2016; Singh & Chatterjee, 2017). Typically, an SLA should cover at least the following areas (Kandukuri et al., 2009):

- Services delivered
- Performance management
- Problem management
- Roles and responsibilities
- Legal & regulatory compliance
- IPR
- Security
- Disaster recovery and business continuity
- Termination

Additionally, a more specific Security Service Level Agreement (SecSLA) can be drawn up, which is a documented high-level agreement between the CSP and the customer, which defines the needed security requirements, related roles and

responsibilities, and how they are enforced and monitored (Kandukuri et al., 2009; Luna et al., 2015; Morsy et al., 2016). To achieve the most effective outcome, Casola et al. (2016) suggested that SecSLAs should be brought to a cloud application/ component level.

3.3 Visibility and Transparency

Cloud solutions commonly suffer from a lack of transparency, as many CSPs do not provide detailed information about their internal policies, procedures, security measures, or employee privileges (Khalil et al., 2014; Luna et al., 2015; Rizvi et al., 2017). Soms et al. (2022) argue that the lack of transparency may also be partially caused due the fact that cloud technology is still relatively new, resulting in challenges with the maturity level of the cloud infrastructure monitoring tools. Multi-locality is a common characteristic of cloud environments, wherein the cloud infrastructure is often distributed across various geographical locations, enhancing the efficiency and availability of cloud services (Rao & Selvamani, 2015; Singh & Chatterjee, 2017). Cloud users often lack awareness of the exact location of where their data is being stored, where is it processed, and from where can it be accessed, which can result in various challenges and concerns (Avram, 2014; Jansen, 2011; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010). Local laws, regulations, and internal organizational policies can impose limitations where the data may reside, often influenced by jurisdictional boundaries under which the data falls. (Avram, 2014; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010). Once data crosses national borders, ensuring its protection under foreign laws and regulations can be challenging (Jansen, 2011).

Data is stored outside the organization's physical boundaries when organizations adopt cloud solutions, and they lose full control over the data. (Singh & Chatterjee, 2017). This causes an issue, as without adequate visibility, the organization cannot ensure that sufficient security controls have been implemented (Duncan, 2020). Take traditional in-house IT environment as an example. To effectively address IT and security risks, system administrators should not be the only ones to have visibility and understand the IT resources and risks related to them (Rizvi et al., 2017). Organizations need to have visibility to the cloud infrastructure, related information assets, processes and a full confidence on what data do they have, where it is stored, how it is protected, how it can be accessed and used, and who has access to it (Duncan, 2020; Jansen, 2011; Rao & Selvamani, 2015; Rizvi et al., 2017; Subashini & Kavitha, 2010).

Security capabilities and service levels typically vary among the CSPs, and while leading vendors might have heavily invested in their security infrastructure and have implemented state-of-the-art security controls, some CSPs lack even the basic native security controls (Duncan, 2020). When

organizations adopt cloud solutions, the baseline for cloud security requirements should align with the organization's existing security standards, aiming to either maintain or exceed the current level (Duncan, 2020; Khan & Al-Yasiri, 2016). To accomplish this, the organization must first assess the native security controls of the cloud and whether the cloud solution complies with the organization's security policies and possible relevant regulatory requirement (Duncan, 2020; Singh & Chatterjee, 2017). This typically requires a standardized and systematic method for evaluating the security measures of the CSP (Duncan, 2020). Cloud solutions are complex systems and include diverse security domains and aspects which need to be considered (Carrera, 2022). Auditability is one of the fundamental aspects of cloud security, and implementing security audits for each deployment layer at each stage of the cloud service lifecycle is crucial for ensuring the cloud solution's security and reliability (Carrera, 2022; Khalil et al., 2014; Torkura et al., 2021). In general, the audit plan should include at least the following aspects (Carrera, 2022; Singh & Chatterjee, 2017):

- encryption and key management
- identity and access management
- device level security
- security logging
- contractual agreements

A common challenge is that especially the leading CSPs are usually reluctant to disclose sensitive and specific information about their security arrangements (Carrera, 2022; Singh & Chatterjee, 2017). However, completely refusing to communicate about the present security arrangements to the customer may backfire, and typically the CSPs tend to rely on independent third-party attestations like ISO 27001 certification in order to offer a certain level of assurance to their customers (Carrera, 2022; Khalil et al., 2014; Luna et al., 2015). Nonetheless, these general attestations do not assure flawless security of the cloud service (Carrera, 2022; Singh et al., 2016).

With the IaaS model, the audits can be extensive because the customers have control over most of the environment (Carrera, 2022). Conversely, in the SaaS model, where customers have minimal control over the cloud environment, audit scope tends to be much more limited (Carrera, 2022). The PaaS model falls somewhere in between (Carrera, 2022). If the native security controls provided by the CSP do not align with the organization's security policies and risk appetite, additional security controls should be implemented by either the CSP or by the organization as a part of the deployment (Duncan, 2020).

3.4 Multi-tenancy and Virtualization

Multi-tenancy is one of the key characteristics of cloud computing, enabling the sharing of cloud resources among multiple organizations and users (Morsy et al., 2016; Rizvi et al., 2017; Rao & Selvamani, 2015; Zissis & Lekkas, 2012). However, the sharing of cloud resources among customers also raises significant security concerns (Arora et al., 2017; Rizvi et al., 2017; Singh et al., 2016). The virtualization layer is critical for cloud computing but at the same time, it is considered as one of the most vulnerable areas for attacks in cloud environments (Khalil et al., 2014; Singh & Chatterjee, 2017). Virtualization vulnerability threats refer to the risks and vulnerabilities associated with the virtualization layer, which facilitates the creation and management of VMs in cloud environments and can be exploited by the attackers (Chauhan & Shiaeles, 2023).

The tenants are isolated from each other at a virtual level but share the resources at hardware level (Singh et al., 2016; Subashini & Kavitha, 2010 Zissis & Lekkas, 2012). The hypervisor is a crucial component of the virtualization layer, responsible for creating and managing the VMs residing above the physical layer of the cloud infrastructure, as well as isolating them from each other and allocating physical computing resources for them to utilize (Coppolino et al., 2017; Singh & Chatterjee, 2017). The hypervisor holds the highest privileges over the VMs and resources it manages, making it essential to protect the hypervisors from attackers (Coppolino et al., 2017).

Typical examples of virtualization attacks include VM escape attacks, VM side-channel attacks, and VM rollback attacks. In a VM escape attack, the attacker manages to bypass the isolation mechanisms of the hypervisor and escapes the guest VM he has access to, compromising the hypervisor, and gaining full control over any resource on the host system, leading to potentially catastrophic impacts on the virtualization infrastructure (Coppolino et al., 2017; Jansen, 2011; Singh & Chatterjee, 2017). In a VM side-channel attack, the attacker controls his own VM on the same physical hardware as the victim's VM and alternates execution with it, enabling the attacker to potentially monitor the data flow and traffic of the victim VM (Khalil et al., 2014; Singh & Chatterjee, 2017). In a VM rollback attack, the attacker exploits previous snapshots of the VM taken with the hypervisor, using them for potentially malicious purposes without the VM owner's awareness, and then restores the VM to its original state to conceal any suspicious activities (Khalil et al., 2014). For example, if the number of failed login attempts for a VM is limited, the attacker could reset the VM after reaching the maximum number of failed attempts, allowing him to continually try different credentials (Khalil et al., 2014).

To address the risks related to virtualization vulnerabilities and prevent the abuse of the cloud service and unauthorized access to neighbor VMs, it is critical for CSPs to ensure that no user system can attain administrative access to the hardware level (Chauhan & Shiaeles, 2023; Rizvi et al., 2017; Singh et al., 2016; Soms et al., 2022). The VMs and hypervisors need to be regularly updated with the latest security patches (Chauhan & Shiaeles, 2023). Additionally, special care must be taken when designing VM lifecycle management processes, managing VM image repositories, sharing VM images, and setting up virtual networks, authentication controls, access restrictions, and resource allocation (Chauhan & Shiaeles, 2023; Jansen, 2011; Singh & Chatterjee, 2017). Network segmentation, VLANs, and virtual firewalls can be implemented to prevent unauthorized access between VMs (Chauhan & Shiaeles, 2023; Jansen, 2011).

3.5 Network Security & Cryptography

One key characteristic of the cloud is that the data and services in the cloud are available to be accessed over the network (Mell & Grance, 2011; Morsy et al., 2016), making network security an essential part of cloud security. For the cloud solutions to work, the data used and stored in the cloud must be transferred between the various cloud resources, services, and endpoints, which depend on each other (Singh & Chatterjee, 2017). Internet and other networks serve as carriers to transfer cloud data from source to the destination, thereby exposing the transferred data to the same threats and vulnerabilities present on the internet and other networks (Gururaj et al., 2017; Singh & Chatterjee, 2017). In fact, many CSPs utilize network security techniques similar to those commonly employed with networks in general, such as firewalls, intrusion detection systems (IDS), and anti-virus gateways (Coppolino et al., 2017). The physical infrastructure of the cloud forms the foundation for cloud environments, and it is located within the data centers of the CSP which need to be well protected against physical and environmental threats of external and internal origin (Singh & Chatterjee, 2017). The data centers function as the first line of defense for the cloud architecture and need to have high level of physical security and strict surveillance implemented (Coppolino et al., 2017).

Network attacks can be either internal or external origin and they can target both virtual and physical networks (Singh et al., 2016; Singh & Chatterjee, 2017). Denial of Service (DoS) attack is a typical example of network based attacks related to cloud computing, where the attacker overwhelms the victim's machine with a large volume of requests through the network, aiming to exhaust the cloud service's computing resources (Jansen, 2011; Kalaiprasath et al., 2017; Singh & Chatterjee, 2017). This can affect the availability of the service, but also the system’s behavior (Singh & Chatterjee, 2017). A Distributed Denial of Service (DDoS) attack is similar to a DoS attack but is more complex and difficult to detect (Singh & Chatterjee, 2017). In a DDoS attack, the attacker

takes over several vulnerable hosts and uses them as a botnet to launch numerous DoS attacks against the victim's machine (Jansen, 2011; Singh & Chatterjee, 2017). Compared to traditional IT systems, the scalability and rapid elasticity of cloud services make them more resilient against DoS and DDoS attacks, as they can adjust the amount of computing resources provided in response to current demand (Coppolino et al., 2017). Different DoS/ DDoS defense solutions can be deployed to detect and counter the attacks, such traffic monitoring, load balancing, flow control, and filtering mechanisms (Butt et al., 2022; Coppolino et al., 2017).

In general, CSPs need to protect the internal traffic of the cloud infrastructure (Coppolino et al., 2017). This involves protecting the traffic between the VMs and traffic originating from outside, while also aiming to minimize the number of access points (Coppolino et al., 2017; Morsy et al., 2016). Cloud resources are typically accessed over the internet through web browsers (HTTP/ HTTPS), remote connections (VPN, FTP), and SOAP, REST, and RPC protocols for web services and APIs (Morsy et al., 2016). Security controls should focus on addressing vulnerabilities associated with relevant protocols to prevent sensitive information to be compromised (Morsy et al., 2016). All data transferred over the network should be secured using strong network traffic encryptions such as Transport Layer Security (TLS), which is a communication protocol that encrypts data between servers, applications, users, and systems (Amazon Web Services, 2024c; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010; Xiaojun & Qiaoyan, 2010). Secure Sockets Layer (SSL) is the predecessor of TLS but is deemed as a legacy technology and is known to have certain security vulnerabilities (Amazon Web Services, 2024c; Sun, 2018).

Securing data transmission over networks is a significant issue itself, which is further complicated in cloud environments where ensuring protection of traffic does not only require protecting the traffic between users and hosts, but also from host-to-host due to the absence of physical connections (Zissis & Lekkas, 2012). Data encryption is a key factor for information security, and cryptographic techniques are used to protect data confidentiality and integrity in the cloud (Arora et al., 2017; Butt et al., 2022; Morsy et al., 2016; Zissis & Lekkas, 2012). The basic idea of cryptography is that it encrypts plain text data into cipher text, which can be decrypted back to plain text using an encryption key (Butt et al., 2022; Singh & Chatterjee, 2017). Encryption algorithms used in encryption can be classified as either being symmetric or asymmetric by nature (Arora et al., 2017; Morsy et al., 2016; Xiaojun & Qiaoyan, 2010). Utilizing a combination of asymmetric and symmetric cryptographic techniques can provide the efficiency of symmetric cryptography while preserving the security level associated with asymmetric cryptography (Deyan & Hong, 2012; Xiaojun & Qiaoyan, 2010; Zissis & Lekkas, 2012).

In the scope of information systems, a Trusted Third Party (TTP) offers scalable end-to-end security services, adhering to standards and adaptable across

various domains, geographical locations, and specialized sectors (Gururaj et al., 2017; Zissis & Lekkas, 2012). More specifically, in cryptography a TTP serves as an optimal security facilitator in cloud environments, enabling secure interactions between two parties that lack prior knowledge of each other, but trust the TTP (Singh et al., 2016; Zissis & Lekkas, 2012). TTP can establish the necessary trust between the interacting parties by ensuring that they are indeed who they claim to be and have undergone a certification process, adhering to a specific set of policies and requirements (Zissis & Lekkas, 2012).

TTPs are linked through certificate paths to establish a web of trust, forming the foundation of Public Key Infrastructure (PKI), which provides reliable ways to implement strong authentication, authorization, data confidentiality, data integrity, and non-repudiation (Zissis & Lekkas, 2012). PKI-based SSO mechanisms are indispensable in cloud environments, as they enable seamless, transparent, and strong authentication across cloud resources, enhancing the security and usability of the cloud infrastructure (Zissis & Lekkas, 2012).

The security of cryptographic controls relies on the management of access to private keys, often referred as key management (Butt et al., 2022; Zissis & Lekkas, 2012; Xiaojun & Qiaoyan, 2010). Key management is a serious concern, and the major issue of key management is how to securely create, storage, access and exchange keys (Esposito & Castiglione, 2016; Morsy et al., 2016). An efficient key management system is essential to maintain records of key holders and revoking keys that are no longer in use (Deyan & Hong, 2012; Esposito & Castiglione, 2016).

3.6 Web Application & API Security

With one of the key characteristics of cloud computing being broad network access, it means that the data and services in the cloud are available to be accessed over the network with standard protocols and devices (Mell & Grance, 2011). Cloud services are typically accessed and managed over the internet using web-based agents such as mobile applications and web browsers, which all may have their own vulnerabilities and weaknesses (Khalil et al., 2014; Morsy et al., 2016; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010). Generally, web applications consist of a front end, back end, and various platforms and frameworks, all crafted and coded by different developers using diverse programming languages, each potentially introducing different types of vulnerabilities (Singh & Chatterjee, 2017; Singh et al., 2016). The security issues and vulnerabilities of web applications in the cloud do not significantly differ from those of other web application technologies (Subashini & Kavitha, 2010).

Web browsers serve as critical components for numerous cloud applications, and organizations should ensure that they are regularly updated with the latest security patches, also covering the various plugins and extensions available, which often aren't included in the automatic updates (Jansen, 2011). Secure

Software Development Lifecycle (SDLC) processes should be followed when developing and implementing web applications (Morsy et al., 2016). Open Web Application Security Project (OWASP) maintains a list of the most critical identified threats to web applications called the "*OWASP Top Ten*" for organizations and software developers to utilize when assessing or developing the security of web applications (OWASP, 2024b).

Application Programming Interfaces (APIs) serve as bridges between different software components, enabling communication and data sharing among them (Chauhan & Shiaeles, 2023). They are essential components of user access to information resources, serving as node points for communication and data processing (Qazi, 2023). Cloud APIs are a common and increasingly used method to access sensitive data and applications, located on the top layers of the cloud framework (Qazi, 2023; Singh & Chatterjee, 2017). However, API developers tend to often prioritize functionality and speed over security features, resulting in many APIs being inherently insecure (Qazi, 2023). This unfortunate combination makes APIs a tempting target for the attackers (Qazi, 2023). Qazi (2023) discovered that organizations tend to lack resources and training to educate user about APIs, with many also being unaware of the APIs they are using and instead relying on third-party providers to manage their API infrastructure. Such practice can lead to opaque API design and third-party providers mishandling their customers' APIs (Qazi, 2023).

The security of cloud APIs is a key component for the present web applications (Gururaj et al., 2017; Singh & Chatterjee, 2017; Qazi, 2023), and security vulnerabilities associated with APIs, such as lack of authentication and encryption, can lead to API attacks (Qazi, 2023). SQL Injection and Cross-site Scripting (XSS) are among the most common type of API injection attacks due to the extensive attack surface (Qazi, 2023). Sanitizing the data of API requests, validating input, using character escaping and filtering, and limiting response data can mitigate the risk of API injection attacks (Qazi, 2023). In Distributed Denial of Service (DDoS) attack, the attacker floods the server with network traffic to overwhelm API memory and restrict users from accessing online services and connected sites (Qazi, 2023). Man-in-the-middle (MITM) attacks are a common type of attack, wherein the attacker intercepts the traffic between a client and a server, enabling the attacker to tamper the communication or eavesdrop on confidential information (Qazi, 2023). MITM attack could for example be carried out by issuing an API request to an HTTP header between a session token (Qazi, 2023). Measures to mitigate DDoS attacks include limiting rate and payload size of incoming traffic, and encryption of the traffic is an effective way to mitigate MITM risks (Qazi, 2023).

Securing APIs can be a difficult task, and many organizations still lack awareness of how to protect APIs from attacks, or even how many APIs they have (Qazi, 2023). The majority of APIs are deployed using API gateways, which among other functions serve the purpose of security gateways and are typically used especially for authentication and monitoring purposes (Red Hat,

2024). The basic principle of a security gateway is similar to firewalls, providing protection for the cloud environment, users, and applications from external malicious network traffic (Qazi, 2023). Robust authentication, authorization, and encryption controls are essential to ensure that only authorized entities can access to particular API functions and resources (Chauhan & Shiaeles, 2023; Kalaiprasath et al., 2017; Qazi, 2023). Indicators of suspicious activity such as potential breaches and unauthorized access attempts should be actively monitored through comprehensive monitoring and logging systems, which capture and analyze API activity (Chauhan & Shiaeles, 2023). Open Web OWASP maintains a list of the top 10 API security risks (OWASPa, 2024) and provides guidance on mitigating them, offering organizations a framework to address the most critical security issues associated with APIs (Qazi, 2023).

3.7 Identity Management and Access Control

Information security and privacy are a growing concern for organizations, with unauthorized access to information resources in the cloud emerging as major issue (Jansen, 2011). Identity management (IDM) is an administrative process focusing on verifying the identities of users and cloud objects within a system and controlling access to the systems resources (Morsy et al., 2016; Singh & Chatterjee, 2017; Subashini & Kavitha, 2010; Sun, 2018). It forms the core for security of the systems and includes three main phases for the verification process which are identification, authentication, and authorization (Morsy et al., 2016; Sun, 2018). IDM and access control overlap with each other, but have distinct focuses, as IDM focuses more on authentication, while access control primarily addresses authorization (Sun, 2018). Cloud platforms should offer a robust and reliable native IDM system ensuring comprehensive coverage of all cloud resources and users, or alternatively support the effective implementation of external IDM systems (Morsy et al., 2016)

Authentication can be defined as the process of verifying the identity of a system or an individual (Singh & Chatterjee, 2017; Zissis & Lekkas, 2012). It serves the purpose of preventing unauthorized access to information resources and can be carried out through various methods such as using passwords, tokens, certificates, or biometrics (Butt et al., 2022; Singh & Chatterjee, 2017; Xiaojun & Qiaoyan, 2010). Authorization again can be defined as the process of permitting or rejecting access to individuals or systems, after they have been authenticated (Singh & Chatterjee, 2017). Strong authentication is critical for cloud security, as weak or insufficient authentication methods can result in unauthorized access to the cloud resources (Singh et al., 2016; Zissis & Lekkas, 2012). Relying solely on traditional passwords for authentication presents vulnerabilities, as stolen passwords can quickly lead to breaches. Multifactor authentication has become a popular method to mitigate the risk by requiring one or more authentication factors beyond the password (Butt et al., 2022).

Another common authentication method in cloud environments is utilizing certificates, which requires a certification authority to validate entities involved in interactions, including servers, devices, and users (Zissis & Lekkas, 2012). This ensures that all physical and virtual entities are provided with the necessary strong credentials, establishing specific boundaries for the cloud's security domain (Singh et al., 2016; Zissis & Lekkas, 2012).

Most organizations utilize Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory (AD) servers to manage user credentials, authentication, and authorization (Singh & Chatterjee, 2017; Subashini & Kavitha, 2010), and the servers can be located either within or outside the cloud environment (Singh & Chatterjee, 2017). Managing multiple user credentials separately within a cloud environment can become overwhelming and risky, particularly when organizations use multiple cloud solutions (Jansen, 2011). Recognizing this challenge, CSPs often permit customers to integrate their LDAP or AD servers with the cloud service, streamlining credential management and enhancing security (Subashini & Kavitha, 2010). This usually involves adopting Single-Sign-On (SSO), enabling users to avoid repetitive authentication processes for each service by utilizing a single strong authentication method that grants them access to services across trusted parties (Singh & Chatterjee, 2017; Zissis & Lekkas, 2012). Utilizing certificates in combination with SSO and LDAP creates a strong authentication process for cloud environments without significantly hindering user mobility and flexibility (Zissis & Lekkas, 2012).

In addition to authentication, effective identity management requires the ability to adjust user privileges and retain control over resource access (Jansen, 2011). Access control allows organizations to enforce specific restrictions for their data stored in the cloud (Butt et al., 2022). The basic principle of access control is that authorized users can access the data, while unauthorized users are restricted from altering or accessing data without permission (Butt et al., 2022). Organizations should design and enforce strict access control policies to determine who can access the data and how (Rao & Selvamani, 2015; Soms et al., 2022). CSPs in the other hand should be able to accommodate their customers' access control policies, which in a multi-tenant environment demands flexibility from the cloud system (Singh et al., 2016; Subashini & Kavitha, 2010). Efficient access management capabilities are essential in the cloud, where data often needs to be accessed by multiple users with varying privileges that may require adjustments over time (Singh & Chatterjee, 2017; Xiaojun & Qiaoyan, 2010). Managing user credentials and privileges efficiently in the cloud can be a complex task, and failure to do so can result in loss of control (Singh & Chatterjee, 2017).

One of the most significant security threats in cloud computing is the hijacking of accounts, services, and traffic (Alassafi et al., 2017; Chauhan & Shiaeles, 2023). Cloud account hijacking occurs when an attacker gains unauthorized access to

an individual's or organization's cloud account, allowing the attacker to conduct malicious activities (Arora et al., 2017; Butt et al., 2022; Chauhan & Shiaeles, 2023). This form of identity theft involves the attacker taking control of the victim's account, which may be further exploited to gain access to other accounts or areas in the cloud environment (Butt et al., 2022; Chauhan & Shiaeles, 2023; Coppolino et al., 2017). In the worst case-scenario, the attacker could gain access to administrative accounts, potentially leading to the loss of the entire service (Gururaj et al., 2017). The attacker could also capture the activities and sensitive transactions in the cloud environment and manipulate the data for example to return forged information to other users or direct them to malicious sites (Arora et al., 2017; Chauhan & Shiaeles, 2023; Singh & Chatterjee, 2017).

Raising awareness of phishing and social engineering threats for the users of the cloud, implementing robust authentication mechanisms such as MFA, enforcing the use of strong passwords, and regularly updating them can mitigate the risk of account hijacking (Butt et al., 2022; Chauhan & Shiaeles, 2023; Kalaiprasath et al., 2017; Khan & Al-Yasiri, 2016). Strategies to mitigate the risk of service threats include regularly patching and updating cloud services to address known vulnerabilities, as well as applying robust network and application-level firewalls to prevent unauthorized access to services (Chauhan & Shiaeles, 2023). To mitigate traffic related risks, network communications can be encrypted by employing secure communication protocols such as HTTPS or TLS (Chauhan & Shiaeles, 2023).

3.8 Human Factors

Singh et al. (2016) stated that humans are the root cause of all issues, but humans can also solve all issues. Employees might use cloud services every day without understanding how the system works or what kind of security precautions should be taken into account (Walterbusch et al., 2017). Cloud security awareness trainings and guidance materials can help to mitigate this risk and enhance the security culture of the organization (Alassafi et al., 2017; Walterbusch ym., 2017). Cloud computing also still suffers from the lack of skilled staff, and it is crucial for both the CSPs and organizations to support continuous education and training to develop expertise in cloud security (Soms et al., 2022).

Social engineering refers to an attack that targets and exploits human vulnerabilities (Bullée et al., 2018; Wang et al., 2021), and it can be viewed as a manipulation technique that employs persuasion principles to trick the victim into complying with the attacker's request, causing the victim to fall for a malicious scam and allowing the attacker to bypass technical safeguards (Bullée et al., 2018; Gupta et al., 2017; Siddiqi et al., 2022; Sun, 2018; Wang et al., 2021). Social engineering based attacks have been a growing problem since the 1970s,

compromising both individuals and organizations (Gupta et al., 2016; Siddiqi et al., 2022; Wang et al., 2021). The goal of the attacks might be for example to obtain confidential data or gain unauthorized entry to physical locations such as data centers, breach computer systems and networks, or otherwise compromise the confidentiality, integrity, or availability of information and information systems such as cloud environments (Bullée et al., 2018; Siddiqi et al., 2022; Wang et al., 2021).

Lastdrager (2014) conducted a comprehensive systematic review about the definition of phishing resulting in a consensual definition: "*Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target*". Phishing is categorized as a form of semantic attack and is typically classified into two main types: malware-based and social engineering based attacks (Arachchilage et al., 2016; Gupta et al., 2016). Phishing attacks are considered to be among the most effective online attack methods that rely on social engineering techniques to deceive victims into disclosing their personal or confidential information (Ebot, 2018; Gupta et al., 2016; Gupta et al., 2017; Khalil et al., 2014; Lance & Jevans, 2005, p. 33; Siddiqi et al., 2022). Despite technological advancements, social engineering-based attacks like phishing remain as a growing problem for cloud security as attackers exploit human vulnerabilities to bypass technical safeguards (Albladi & Weir, 2020; Gupta et al., 2016; Schaab et al., 2017; Siddiqi et al., 2022).

Cyber security researchers and practitioners primarily suggest on two main approaches to mitigate the risk of social engineering based attacks like phishing: implementing technical safeguards and promoting security awareness (Bullée et al., 2018; Gupta et al., 2016; Wright & Marett, 2010). Technical safeguards typically include automation, such as anti-phishing filters and alerts, while enhancing security awareness involves educating users, which many studies have found to be effective (Sur, 2018; Wright & Marett, 2010).

Malicious insider threats are another human based threat in cloud security, involving individuals who have authorized access to cloud resources but intentionally misuse their position for harmful purposes (Butt et al., 2022; Chauhan & Shiaeles, 2023; Singh & Chatterjee, 2017). Malicious insiders are considered as a major threat to cloud security, with the level of impact depending on their access rights and their ability to infiltrate organizations and their assets (Khalil et al., 2014; Rizvi et al., 2017; Soms et al., 2022). A significant portion of data breaches are caused by insiders, who are typically either CSPs or the cloud customer's current or former employees, contractors, partners, or service providers (Butt et al., 2022; Chauhan & Shiaeles, 2023; Singh & Chatterjee, 201; Soms et al., 2022). These individuals have been granted access to the cloud environment and may possess insider knowledge of its security arrangements (Butt et al., 2022; Chauhan & Shiaeles, 2023; Jansen, 2011; Singh & Chatterjee, 2017).

To mitigate the risk of malicious insiders, organizations should implement strict access control measures, adhere to the principle of least privilege, and

establish robust IAM mechanisms and policies (Chauhan & Shiaeles, 2023). Robust monitoring and auditing systems can be utilized to track user activities and system events, as well as to report any detected anomalies (Chauhan & Shiaeles, 2023). Enforcing segregation of duties is crucial to ensure that individual employees do not hold disproportionate control or privileges over the cloud environment or critical processes (Chauhan & Shiaeles, 2023). Comprehensive screening processes are recommended during recruitment, especially for roles involving critical responsibilities or extensive administrative privileges (Gururaj et al., 2017).

3.9 Incident Management and Forensics

Robust security incident management processes and controls are essential for effective threat detection and response (Duncan, 2020). Organizations should design and implement comprehensive incident management policies and procedures, leveraging monitoring and analytics throughout the cloud to identify threats, vulnerabilities, and configuration weaknesses (Duncan, 2020; Esposito & Castiglione, 2016). Due to the complexity of cloud environments and the massive amount of log data produced, real-time monitoring of threats and vulnerabilities become difficult if not impossible for humans to process by themselves, which is why automation is required to support the efficient threat detection and response processes (Khalil et al., 2014; Qazi, 2023).

Intrusion Detection Systems (IDS) are applications or devices designed to monitor and analyze system activities and network traffic, identifying and reporting any detected anomalies and suspicious behavior (Butt et al., 2022; Khalil et al., 2014). However, studies show that traditional IDS are not optimal for cloud environments (Qazi, 2023). Security Information and Event Management (SIEM) systems are a more common security solution used within cloud environments, and it can be used to support the monitoring and analysis of real-time network events, issuing alerts based on learned patterns of normal and abnormal behavior within the network, and reacting to them based on set rules (Singh & Chatterjee, 2017).

Most SIEM systems and some of the IDS leverage Machine Learning (ML), which is an extension of convolution neural networks (CNNs), enabling devices or systems to learn and make decisions by training them with relevant data (Qazi, 2023; Subramanian & Tamilselvan, 2019). This equips the system to handle diverse scenarios and make intelligent decisions (Subramanian & Tamilselvan, 2019). ML provides a fast and efficient way to analyze data, enabling detection of various threats and abnormal behavior more effectively than traditional security methods (Qazi, 2023). However, deploying ML based cloud security systems is a challenging and laborious task due to the substantial amount of training data required, and integrating new data forms requires intensive training efforts (Subramanian & Tamilselvan, 2019). Regular tuning of

the system is also essential to ensure its capability to detect new anomalies within the network and its boundaries (Subramanian & Tamilselvan, 2019).

As cybercrime poses a major threat to organizations today, particularly as more and more of the business and daily operations are relying on network applications such as cloud applications and devices (Singh et al., 2016). Digital forensics is no longer a niche process solely for the use of the officials, but it plays a vital role in organizations across both public and private sectors to investigate cybercrime and computer-assisted crime (Singh et al., 2016). Different kind of digital forensic tools and techniques can be used to for collecting and examining digital evidence from disk images, logs, image files and snapshots, memory dumps, endpoint devices and such, and ensuring that the evidence remains forensically sound (Esposito & Castiglione, 2016; Singh & Chatterjee, 2017; Singh et al., 2016). Due to the complexity and dynamic nature of the cloud, applying digital forensic tools can be more challenging compared to traditional in-house IT environments, as the data is often moved between locations in the cloud rather than being stored in a static physical storage location (Singh & Chatterjee, 2017). To ensure the efficiency of cloud forensics, sufficient expertise and understanding of the domain is required from both the CSP and the cloud customer, depending on the deployment model and SLAs (Singh & Chatterjee, 2017).

4 RESEARCH METHODOLOGY

In a university context, according to Myers (2020, p. 6) research can be defined as *"an original investigation undertaken in order to contribute to knowledge and understanding in a particular field"*. This research should generate new knowledge, ensuring that the related facts, their interpretations, or the theories used to explain them are novel in the particular field in question. To ensure that the research results are robust and novel, the findings must be subjected to scrutiny and formal evaluation by experts qualified in the field. This evaluation process, known as the peer review system, is present in all scientific disciplines and distinguishes science from other human endeavors, ensuring that the research must comply with certain standards before it can be published. Research is typically carried out by individuals who have specialized knowledge of the topics, theories, and methods to their field. This research can be empirical or conceptual in nature and in fields like computer science or information systems science, it may also involve the experimental design of new or enhanced materials, devices, products, or processes. Since the subject matter, theories, and methods used in a particular field can evolve over time, scholars typically demonstrate their understanding and familiarity with the latest knowledge by writing literature reviews that cover recent relevant research. (Myers, 2020, p. 6-7)

In business and management, research focuses on topics pertinent to its own disciplines, such as management strategy, finance, human resources, logistics, information systems, marketing, and operational management. It often integrates research from other fields like statistics, psychology, and sociology. Balancing rigor and relevance is a persistent challenge for researchers in business and management. Business schools have faced criticism for prioritizing rigor at the expense of relevance in their research. Rigor in research is often defined as adherence to the standards of scientific research, including following the scientific research model, undergoing peer review, and being published in an academic journal. However, academic research business journals are often criticized for being too theoretical and not sufficiently

practical for business professionals. Then again, relevance in research is often characterized by having direct implications for business and management, with results that can be immediately applied or deployed by the business professionals. The downside of relevance in research is that it often comes with little theoretical contribution and is seen more similar to consulting, and therefore often fails to comply with the standards of scientific research. (Myers, 2020, p. 12-14)

The following subchapters describe the research methodology used in the thesis, and the motivation for their selection. First, quantitative and qualitative research methods are introduced in general, followed by a description of the research methods chosen for the thesis. Finally, the implementation of the research and the data collection methods are introduced.

4.1 Research Methods

Research methods are often classified as quantitative or qualitative. Quantitative methods, developed to study natural phenomena, include survey methods, laboratory experiments, formal methods, and numerical techniques such as mathematical modelling. One of the key characteristics of quantitative research include the use of statistical tools to analyze numerical data. Qualitative research methods were developed to study social and cultural phenomena and include approaches such as action research, case study research, and grounded theory. Data sources for qualitative research can include observations, interviews, questionnaires, documents and texts, as well as the researcher's own impressions and reactions. Qualitative data primarily focuses on what people have said, helping us understand their motivations, actions, and the environments in which they work and live. (Myers, 2020, p. 8-9)

Quantitative research is generally more suitable for large sample sizes and generalizing results to broader populations. It is ideal for situations where researchers aim to study a specific topic across numerous individuals or organizations to identify trends or patterns. In business and management, the primary limitation of quantitative research lies in its tendency to overlook a majority of the social and cultural factors within organizations. The context is often overshadowed by the emphasis on generalizing findings across a population. Qualitative research is better suited for studying social, cultural, and political characteristics of individuals and organizations, as well as in-depth exploration of specific subjects, making it ideal for cases where the topic is novel and has not been extensively researched before. However, a well-known challenge with qualitative research methods is the difficulty in generalizing findings to a larger population. (Myers, 2020, p.9-10)

Literature review is research method in which past research is studied and summarized to conduct a descriptive synthesis that can act as a base for future research findings (Mandal & Khan, 2021; Salminen, 2011). As a research method it can be considered as a mixed method since it can combine elements from both quantitative and qualitative research (Salminen, 2011). The emphasis placed on either approach depends on whether the literature review is conducted with a more descriptive and qualitative focus or a more statistical and quantitative orientation (Salminen, 2011). The literature review is typically situated in the introduction section of a study, making it commonly perceived as a supportive research method and technical phase aimed at presenting past research relevant to the study (Mandal & Khan, 2021; Salminen, 2011).

Triangulation proves valuable when researchers aim to examine a topic from various perspectives, enhancing their comprehensive understanding of the subject. This can be accomplished by employing multiple research methods, using multiple techniques to collect data, or by integrating both qualitative and quantitative research methods within a single study. In qualitative research, triangulating data is often necessary. For example, this might involve cross-referencing data from interviews or surveys with information extracted from documents and texts, or with data collected through various research methods. (Myers, 2020, p. 10-11)

In the realm of business and management research, qualitative methods are considered more apt for achieving both rigor and relevance as they facilitate the integration of scholarly insights with practical applications (Myers, 2020, p. 15). To conduct a successful qualitative study, researchers must actively engage with individuals in real-world organizations, recognizing the complexity inherent in organizational dynamics and addressing the often-unquantifiable issues at hand (Myers, 2020, p. 15). Therefore, qualitative research methods were deemed suitable and chosen for this thesis, with the research method being a qualitative case study. A literature review was used to create the knowledge base for the study, while empirical material was collected through a survey targeting experts in cloud services and information security. Triangulation was employed to form the study's findings, combining the results of the literature review and the survey.

4.2 Implementation and Data Collection

The research method for the thesis is a qualitative case study, and the baseline of the study are organizations that use or produce cloud solutions. The aim of the study is to determine how and why organizations should address information security when adopting or using cloud services. One main research question was defined for the thesis, and one sub-research questions to support this, which the study aims to answer:

1) What should organizations take into account regarding information security when deploying and managing cloud services?
   a) What information security risks can the use of cloud services cause for organizations?

The knowledge base for the study was established through a literature review. Approximately 90 academic articles, primarily peer-reviewed, covering topics related to cloud computing, cloud security, and other information technology and cybersecurity areas, were examined. Additionally, relevant publicly available standards, reports, and blogs on cloud computing and cloud security were reviewed. Materials from specialist security forums and major cloud service providers like Amazon Web Services, Google, and Microsoft were also studied (Wright et al., 2023).

Empirical material for the study was gathered through a survey targeting experts in cloud security and information security. An open online survey (Appendix 1) was selected as the method and was distributed to five security-critical large corporations that use and/or produce cloud services, as well as to a specialist security forum with approximately 1,000 highly educated members. An online survey and reporting platform named Webropol was used to design the survey, and completing the survey was estimated to take about 20 minutes. All responses were treated as confidential, with no personal information or background details of the participants being disclosed to third parties. As the subject of the study can be perceived as sensitive in organizations, participating anonymously or without disclosing the background organization was allowed. The survey was available to be participated either in Finnish or English. To encourage participation, a small gift card raffle was also offered.

The survey was divided into ten sections, each on a separate page. Respondents had to complete the questions on the current page before advancing to the next section. The questions were either multiple-choice or free-response. While answering free-response questions was optional (except for those regarding the respondent's background information), multiple-choice questions were mandatory. Multiple-choice questions with predefined options always included the possibility for respondents to add any options they felt were missing from the list.

The first page of the survey was reserved for the cover letter, where respondents were provided with general information about the survey, a brief description of the study's background and subject, and an introduction to the author. The second section of the survey included questions about the respondents' backgrounds, such as their country of presence, work experience, and current job description or area of responsibility. Providing their name and title was optional. The third section included questions about the respondent’s organization: the industry and sector it operates in, whether the organization uses or provides cloud services, and if so, the type of cloud services involved. In

the fourth section the respondents were asked to describe their attitude towards cloud services and assess the benefits of cloud services while given a pre-defined list of the benefits generally associated with the adoption of cloud services when compared to traditional IT systems. In addition, the respondents were asked to briefly describe the most important benefits in terms of risk management and security that they thought is possible to achieve by adopting cloud services. The fifth section of the survey focused on CSPs. Respondents were asked to describe considerations for risk management and security when selecting a CSP, the most important factors in assessing CSP reliability, and how risk management and security should be addressed at the contract level with CSPs. In the sixth section, respondents were asked about the security of cloud solutions. Questions focused on their perceptions of the security level of the cloud services used in their organizations, their ability to influence that security level, and whether their organizations had moved critical data or services to the cloud, restricted cloud usage, or decided against adopting certain cloud solutions due to security concerns.

The seventh section of the survey focused on cloud security risks. Respondents were asked to assess the criticality of security risks typically associated with cloud solutions from a predefined list. The risks were categorized into three different categories: people-related risks, process-related risks, and technology-related risks. At the end of the seventh section, respondents were asked to rate their organization's awareness of security risks related to cloud solutions on a scale from “poorly” to “very well”. The eighth section of the survey focused on the protection of cloud services. Respondents were given a list of predefined security controls typically involved in protecting cloud services and were asked to assess their importance on a scale from "not important at all" to "very important." The security controls were categorized similarly to the previously presented cloud security risks into three different categories: people-related controls, process-related controls, and technology-related controls. At the end of the eighth section, respondents were asked to describe which security controls they see as the most important development areas in their own organization. The ninth section of the survey concentrated on best practices and frameworks. Respondents were asked if their organization uses any of the listed predefined standards, frameworks, and tools for evaluating or developing the security of cloud solutions. This was followed by two questions about how respondents perceived the advantages and disadvantages of such standards and frameworks. Additionally, respondents were asked if their organization's cloud solutions are regularly audited and whether their organization requires any security-related certificates or approvals from the CSPs they use. The tenth page of the survey was reserved for the thank you page, where the respondents were given the opportunity to leave their contact information for either participating to the draw or if they wished that the results of the survey would be shared with them later.

Finally, the results of the literature review were triangulated and synthesized with the survey data to cross-check the information and draw conclusions relevant to the research questions. The survey provided valuable insights into real-world organizations' knowledge and perspectives on the risks associated with cloud services and the necessary security controls to mitigate these risks. The results will help organizations to acknowledge the risks related to the use of the cloud services and define effective security controls to mitigate them.

5 SURVEY RESULTS & ANALYSIS

In the end, 13 respondents completed the online survey, while 78 individuals had opened it and 25 had started but did not submit their responses. Apart from the evident reason that working professionals are often too busy to complete surveys, feedback from respondents suggests that while the study topic was interesting, many found it too complex or technical. This feedback aligns with the claims that organizations lack expertise in cloud security and that the industry continues to face a shortage of cloud security specialists.

The majority (92.3%) of respondents were located in Finland and worked in the security and/or ICT industries within the private sector. All respondents' job duties involved working closely with cloud solutions, with an average of 4.6 years of experience in their current positions, ranging from 1 to 14 years, and a standard deviation of 3.8 years. Additionally, 15.4% of the respondents worked in small or medium-sized organizations (fewer than 250 employees), while 76.9% were employed by large corporations with 500 or more employees.

	Yes	**No**	**Unsure**
Infrastructure as a Service (IaaS)	53,8%	7,7%	38,5%
Platform as a Service (PaaS)	38,5%	15,4%	46,1%
Software as a Service (SaaS)	84,6%	7,7%	7,7%
Something else	0,0%	0,0%	0,0%
Total	**44,2%**	**32,7%**	**23,1%**

Table 1 Used cloud service delivery models.

All respondents indicated that their background organizations use cloud services, with Software as a Service (SaaS) being the most commonly used service delivery model (84%). Infrastructure as a Service (IaaS) was used in 54% of the organizations, while Platform as a Service (PaaS) solutions were used in only 39% of the organizations. Furthermore, 38% of the respondents were unsure if their organizations used IaaS solutions, and 46% were unsure about the use of PaaS solutions. Only 8% of the respondents were unaware if their organizations used SaaS solutions.

Public cloud was the most commonly used deployment model (92%), followed by private cloud (77%) and hybrid cloud (61%) among the respondents' background organizations. Only 8% of the respondents were unsure if their organizations used public cloud, and 15% were unsure about the use of private cloud. However, 31% of respondents were uncertain about the use of hybrid cloud in their background organizations.

	Yes	**No**	**Unsure**
Private Cloud	76,9%	7,7%	15,4%
Public Cloud	92,3%	0,0%	7,7%
Hybrid Cloud	61,5%	7,7%	30,8%
Something else	0,0%	100,0%	0,0%
Total	**57,7%**	**28,9%**	**13,5%**

Table 2 Used cloud deployment models.

69% of the respondents stated that their background organization provides cloud services, with SaaS being the most commonly provided service model (89%). IaaS and PaaS were each offered by only 11% of the organizations providing cloud services. Additionally, 44% of the respondents were unsure if their organizations provided IaaS solutions, and 56% were unsure about the provision of PaaS solutions.

	Yes	**No**	**Unsure**
Infrastructure as a Service (IaaS)	11,1%	44,5%	44,4%
Platform as a Service (PaaS)	11,1%	33,3%	55,6%
Software as a Service (SaaS)	88,9%	0,0%	11,1%
Something else	0,0%	100,0%	0,0%
Total	**27,8%**	**44,5%**	**27,8%**

Table 3 Provided cloud service delivery models

Among organizations providing cloud services, public cloud was the most commonly offered deployment model (78%). Private cloud solutions were provided by 56%, and hybrid cloud by 45% of these organizations. However, 22% of respondents from organizations that provided cloud services were unsure if private or public cloud solutions were offered, and 33% were unsure about the provision of hybrid cloud solutions.

	Yes	**No**	**Unsure**
Private Cloud	55,6%	22,2%	22,2%
Public Cloud	77,8%	0,0%	22,2%
Hybrid Cloud	44,5%	22,2%	33,3%
Something else	0,0%	100,0%	0,0%
Total	**44,5%**	**36,1%**	**19,4%**

Table 4 Provided cloud deployment models.

5.1 Benefits of Cloud Services

Respondents were asked to describe their background organization's attitude towards cloud services on a scale from 1 to 5, where 1 indicates a very cautious attitude and 5 indicates a very open attitude. 77% estimated that their organization's attitude towards cloud services was either open or very open, while 15% of the respondents estimated the attitude as somewhat neutral. Only 8% of respondents indicated that their background organization's attitude towards cloud services was very cautious. Interestingly, when asked about the reasons for this cautious attitude, concerns regarding risks or security issues related to cloud services did not play a significant role. These findings appear to contradict previous studies claiming that many organizations are hesitant to adopt cloud solutions due to security concerns. However, the positive attitude towards cloud computing among the respondents' organizations might be attributed to their predominantly tech-savvy nature. If the empirical data had been collected through interviews with organizations from diverse segments and sizes, without the option for respondents to withdraw or leave answers incomplete as allowed in a survey, the results might have differed in this context.

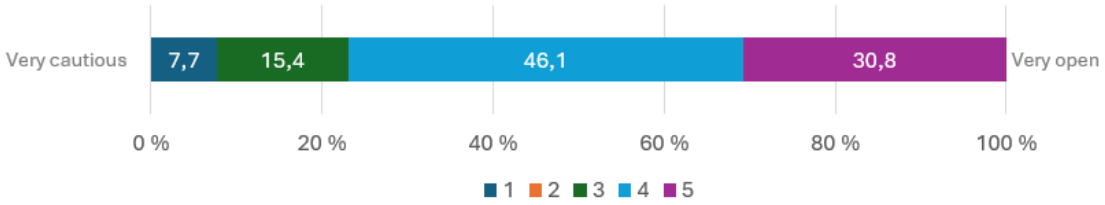

Figure 1 Attitude towards cloud services.

According to the survey, operational reliability and continuity was regarded as the most significant benefit of adopting cloud services compared to traditional information systems. 85% of respondents stated that operational reliability and continuity were very important, while the remaining 15% considered them important. Scalability was seen as very important by 77% of respondents, with 23% stating it was important. Cost-efficiency and accessibility of services were both deemed very important by 54% of respondents and important by 38%. Rapid deployment was considered important or very important by 85% of respondents. Data shareability was perceived as the least important benefit of adopting cloud services compared to traditional information systems, yet 61% of respondents still considered it either important or very important. These findings support the claims from previous research regarding the benefits of cloud computing when compared to traditional information systems.

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Cost-efficiency	0,0%	0,0%	7,7%	38,5%	53,8%	0,0%
Rapid Deployment	0,0%	0,0%	15,4%	53,8%	30,8%	0,0%
Scalability	0,0%	0,0%	0,0%	23,1%	76,9%	0,0%
Data Shareability	0,0%	7,7%	30,8%	38,4%	23,1%	0,0%
Accessibility of Services	0,0%	0,0%	7,7%	38,5%	53,8%	0,0%
Interoperability of Systems	0,0%	0,0%	15,4%	30,8%	46,1%	7,7%
Operational Reliability and Continuity	0,0%	0,0%	0,0%	15,4%	84,6%	0,0%
Something else	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Total	**0,0%**	**1,0%**	**9,6%**	**46,1%**	**46,1%**	**13,5%**

Table 5 Importance of generally associated benefits with the adoption of cloud services compared to traditional information systems.

The respondents were also asked to briefly describe the most important benefits in terms of risk management and security that they believed could be achieved by adopting cloud services. A high level of availability and continuity of services was emphasized, particularly in terms of managing and protecting the physical infrastructure of the environment. The shared responsibility model was also regarded as a significant benefit of adopting cloud services, as it allows organizations to share security responsibilities with the cloud service provider (CSP). Additionally, many respondents highlighted the scalability of cloud services as an important advantage, as well as the extensive tools provided by CSPs to manage the security of the cloud environment.

Responses
The hyper scaler cloud providers are capable of offering so highly available infrastructure that the risk of hardware infrastructure failures are very low. The shared responsibility model of the cloud security is also a great way to improve the security when you don't have to worry about the data center and hardware related security threats.
The physical protection of data is easily managed if you use well-known public cloud service providers. For example, it is easy to store backups in several geographical locations. Well-known public cloud service providers also offer very stable platforms, making it easy to keep system availability at a very high level.
Centralized risk and security management.
Ease of managing access rights. For large trusted CSPs, security and risk management are offered as a standard service. Ready-to-use tools.
Improving information security compared to on-premises solutions.
By using public cloud providers, you get built in security for authentication and authorization. And the infrastructure is also managed by cloud service provider. It is also easier to get overview by using native cyber security tools provided by the cloud services provider. By using cloud provider, you also have automatically a very good inventory of

all your resources, which is important for security also.
Compared to an on-premises service, using a cloud service is more cost-effective and continuity is better secured. Scalability is important vs. on-premises service where more capacity may be acquired at once, and some may remain completely unused.
Secure by design (sometimes), operational reliability and observability.
Local and possibly customer-administered servers can be get rid of, in which case the responsibility for maintaining operations, backups and general security rests with the supplier, who must be familiar with these at a completely different level than the company using the services.
In risk management, the most important benefits are availability and scalability. In terms of security, cloud services offer solutions that are being designed and implemented by several experts.
Flexibility/scalability, high-level if information security, ensuring continuity (backups, fast recovery, etc.) and ease of use.

Table 6 Benefits of cloud services in risk management and security.

5.2 Choosing a Cloud Service Provider

When asked about considerations for risk management and security when choosing a cloud service provider (CSP) and the most important factors for ensuring a CSP's reliability, many respondents emphasized the importance of certifications when assessing the reliability and security capabilities of a CSP. Especially ISO/IEC 27001 certification was highlighted by the respondents, when asked about security-related certificates or approvals required from CSPs by the respondents' background organizations. The respondents also highlighted the importance of visibility and transparency, along with the comprehensiveness of the available documentation, which positively influenced the evaluation of a CSP's reliability. The availability of various tools to manage security was also deemed important. Additionally, well-known larger CSPs were initially perceived to be more reliable and a better option for risk management and security, as they are likely to have more resources and tools to manage cloud security effectively. However, many respondents emphasized that auditing the CSP and testing the offered cloud solution beforehand should always be conducted.

Responses
Rely on the bigger hyper scalers who have the resources to the mitigate the risk and security issues proactively and provide constantly new services for improving on those areas.
Comprehensive documented risk analysis. It is worth finding out the available certifications. Comprehensive testing of the platform before taking it into use.
Known service provider.
Various certifications based on standards serve as a good proof of the reliability of the organization providing cloud services. In general, big global players are more reliable than small local ones. My personal view is that it would still be good to do an audit for a potential cloud service provider in addition to checking certifications.

Technical solution, service levels, competitive price level, technical expertise of the personnel.
You should of course evaluate the provider and what if any certifications they have. Mostly for the physical and infrastructure. It is however a shared responsibility, and you will still have responsibility of the workloads in the cloud. You should therefore also evaluate what if any cyber security tools there are provided by the cloud service provider.
Ensuring continuity of service, duplication of capacity. Provider certification, references.
Alignment with best practices/industry standards. Data handling. Reporting in case of an incident. Compliance. Access management (authentication and access control).
Reputation, level of documentation, transparency and information sharing, certifications.
In my opinion, certificates are the most important factors when choosing providers.
Large enough provider with good references and possibly previous cooperation. Google / Microsoft, for example are not likely to fall and you can always get either free/paid help from them if needed.
Availability, location.

Table 7 Most important factors to ensure the level reliability and security of a CSP.

Many respondents highlighted the importance of SLAs when asked about incorporating risk management and security into contracts with CSPs, which supports the findings of previous studies. It was emphasized that agreeing on the preferred level of security and specific security requirements at the contract level with the CSP is essential, as well as clearly defining roles and responsibilities related to them. Additionally, data protection and privacy requirements were considered important factors to include in the contracts between the organization and the CSP. One respondent also emphasized the importance of avoiding vendor lock-in when finalizing a contract with the CSP, which has also been highlighted in previous research (Chauhan & Shiaeles, 2023; Rizvi et al., 2017; Singh & Chatterjee, 2017).

Responses
There should be a clear definition of the responsibilities as a part of the agreement. AWS has the good example within the shared responsibility model.
You should pay special attention to data protection issues, e.g. because of GDPR. E.g. DPA and DPIA procedures.
Easy to change service provider if desired.
Continuity plans, recovery plans at a minimum
The information security requirements for the service must be accurately described in the contract.
The big cloud service providers will offer more terms of service than individual contracts, but there are service levels, and you should of course choose the service level and or extra services to fulfill your cyber security needs.
SLA, security audits. Address data protection, privacy, and compliance requirements in the contract.
The requirements include regular reporting, a clear delineation of responsibilities and obligations. A difficult question here, but certainly also for the party procuring the service if the company does not already have expertise related to the matter.
SLAs with sanctions for contracts.

Table 8 How should risk management and security be taken into account in contracts with the CSPs.

5.3 Security of Cloud Services

53% of respondents felt that the cloud services used in their background organization had a very good level of security, and 38% considered it to be on a good level. Only 8% felt that the security level was average, with none stating it was bad or very bad. This supports findings from previous research (Singh & Chatterjee, 2017; Torkura et al., 2021) that the increasing adoption of cloud solutions over the years has driven continuous advancements in cloud technology and security. Additionally, 54% of respondents agreed or completely agreed that they feel they can influence the security level of the cloud services used. However, 31% of respondents disagreed or completely disagreed that they had any influence on the security level of their organization's cloud services. This discrepancy could potentially be attributed to the varying roles and responsibilities of the respondents within their organizations. Users of information systems generally have less influence over the security of the system compared to those in administrative roles, for instance.

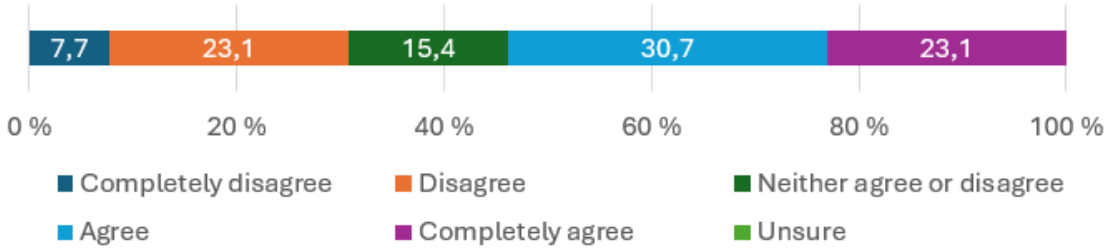

Figure 2 Ability to influence the security level of cloud services in use.

62% of respondents indicated that their background organization has moved critical data or services to the cloud, while the remaining respondents stated that critical data or services had been partly moved to the cloud. Nearly half of the respondents (46%) were unsure if their background organization had chosen not to adopt certain cloud solutions or limit their use due to security concerns. Meanwhile, 8% of respondents answered that security concerns had not affected the adoption or usage of cloud solutions, and 46% stated that their background organization had either decided against adopting some cloud solutions or had limited their usage due to security concerns. Given that 91% of the respondents indicated the security level of the cloud solutions used in their organization is either good or very good, this finding prompts questions about why organizations continue to express hesitations about adopting or using cloud solutions due to security concerns. This could serve as an interesting topic for future research.

5.4 Cloud Security Risks

69% of the respondents stated that their background organization is either well aware (38%) or very well aware (31%) of security risks related to cloud solutions, while 31% answered their background organization to be moderately aware of the risks. None of the respondents rated their background organization to be either poorly or not very well aware of the cloud security risks. As cloud solutions have been widely adopted by organizations for over a decade, this result is unsurprising (Mandal & Khan, 2021). However, it underscores the need to improve awareness of security risks associated with cloud solutions, particularly given that the respondents predominantly worked in technology-oriented organizations.

Regarding cloud security risks related to people, 62% of respondents perceived the lack of security awareness and training as a significant or critical risk. Opinions were divided on data leaks/data loss, with 46% viewing it as a critical risk and the rest considering it as more of a minor risk. Similarly, opinions on malicious insiders were split, with 46% seeing them as a significant or critical risk, while the rest considered them moderate or minor risks. The unauthorized abuse of cloud resources, such as crypto mining and executing DOS attacks, showed the most variation in respondents' perceptions of its risk level in terms of cloud security. Human errors were also mentioned as people-related risk for cloud security that should be taken into account. Based on the results, it can be concluded that security risks associated with people pose a significant threat to cloud security.

	Insignificant	**Minor**	**Moderate**	**Significant**	**Critical**	**Unsure**
Insider risks (malicious)	0,0%	30,7%	23,1%	30,8%	15,4%	0,0%
Lack of security awareness or training	0,0%	15,4%	23,1%	38,4%	23,1%	0,0%
Data leak/ Data loss	7,7%	38,5%	7,7%	0,0%	46,1%	0,0%
Unauthorized cloud resource abuse (e.g. mining crypto, executing DOS attacks etc.)	0,0%	23,1%	30,7%	15,4%	23,1%	7,7%
Something else, what?	0,0%	0,0%	33,4%	0,0%	33,3%	33,3%
Total	**0,0%**	**21,5%**	**23,6%**	**46,1%**	**8,2%**	**13,5%**

Table 9 Significance of people related risks to cloud security.

Among cloud security risks related to processes, identity and access management (IAM) related risks were perceived as the most significant ones. 54% of respondents stated IAM risks to be either a significant or critical risk,

while 38% saw it as a moderate risk. None of the respondents classified IAM risks as a minor or insignificant risk for cloud security. Compliance risks (e.g., risks related to laws and regulations) and risks arising from inadequate contract models in terms of security were highlighted as significant or critical risks by over 40% of the respondents. Similarly, over 40% of respondents considered risks related to backup protection to be either significant or critical. Risk for the organization's business models not supporting the usage of cloud solutions was perceived as moderate by 39% of the respondents, and risks related to data destruction and retention processes were also mostly deemed moderate (46%).

While the roles and responsibilities regarding security were highlighted by the respondents earlier to be an important factor to take into account on a contract level with the CSPs, risks related to data ownership and responsibilities were considered to be significant or critical for cloud security only by 23% of the respondents, while 62% of respondents stated that the risk is only minor or moderate. Risks related to limited visibility of cloud solutions (e.g. location of data, security controls) were not seen as critical by none of the respondents, and 61% of respondents considered them to be either moderate or minor risks, and even insignificant (7%). This contrasts with previous research indicating that one of the primary challenges for cloud computing is the lack of visibility into how data is stored or secured (Carrera, 2022; Singh et al., 2016; Subashini & Kavitha, 2010). Overall, the significance of cloud security risks related to processes varied greatly depending on the specific process. With the exception of risks related to encryption key management, they were generally perceived as either significant, moderate, or even minor threats to cloud security.

	Insignificant	**Minor**	**Moderate**	**Significant**	**Critical**	**Unsure**
Organization's business models do not support cloud solutions	0,0%	15,4%	38,4%	15,4%	7,7%	23,1%
Compliance risks (laws and regulations)	0,0%	30,7%	15,4%	30,8%	7,7%	15,4%
Risks arising from inadequate contract models in terms of security	0,0%	30,8%	7,7%	38,4%	7,7%	15,4%
Risks related to data ownership and responsibilities	0,0%	38,4%	23,1%	15,4%	7,7%	15,4%
Risks related to limited visibility (location of data, security controls)	7,7%	23,1%	30,7%	30,8%	0,0%	7,7%
Identity and access management risks (IAM)	0,0%	30,7%	38,5%	46,1%	7,7%	7,7%

Risks related to encryption key management	0,0%	38,5%	7,7%	23,1%	23,1%	15,4%
Risks related to backup protection	0,0%	7,7%	15,4%	30,8%	15,4%	7,7%
Risks related to data destruction and retention processes	0,0%	15,4%	46,1%	15,4%	7,7%	7,7%
Something else, what?	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Total	**0,8%**	**22,3%**	**22,3%**	**24,6%**	**8,5%**	**21,6%**

Table 10 Significance of processes related risks to cloud security.

Cloud security risks related to technologies were mostly seen as either moderate or significant, though there was some variance in the responses. Denial of service attacks were clearly viewed as the most important technology-related risk for cloud security, with 31% of respondents considering it a critical risk and 39% a significant risk. Risks arising from vulnerabilities in shared technology, system architecture, and virtualization vulnerabilities were mostly seen as either significant or moderate by the respondents.

Risks related to web application vulnerabilities and technical interfaces such as APIs were also deemed important. Web application vulnerabilities were considered a significant risk by 38% of respondents, while technical interface-related risks were deemed significant by only 15%, with 69% viewing them as a moderate risk. Surprisingly, despite availability being a fundamental aspect of information security, service availability issues were considered a minor risk by 39% of respondents, though 15% saw them as a critical risk and 38% as a moderate risk. Compatibility issues between cloud platforms emerged as the most ambiguous technology-related risk, with 31% of respondents unsure of its significance to cloud security. Supply chain risks were also mentioned to be noteworthy in terms of cloud security. Technology related security risks were mostly perceived as a significant or a moderate threat to cloud security, with some variance depending on the risk in question.

	Insignificant	**Minor**	**Moderate**	**Significant**	**Critical**	**Unsure**
Risks arising from vulnerabilities in shared technology	0,0%	23,1%	30,8%	38,4%	7,7%	7,7%
Risks related to system architecture	0,0%	30,8%	23,1%	38,4%	7,7%	7,7%
Risks related to virtualization vul-nerabilities	7,7%	15,4%	23,1%	38,4%	15,4%	15,4%
Risks related to web application vulnerabilities	0,0%	7,7%	53,8%	38,5%	0,0%	0,0%

Risks related to technical interfaces (e.g. API)	0,0%	15,4%	69,2%	15,4%	0,0%	0,0%
Service availability issues	0,0%	38,4%	38,5%	0,0%	7,7%	7,7%
Compatibility issues between cloud platforms	0,0%	30,7%	30,8%	7,7%	30,8%	30,8%
Account, Service, and Traffic High-Jacking	0,0%	23,1%	23,1%	30,7%	15,4%	15,4%
Denial of service attacks	0,0%	15,4%	7,7%	38,4%	7,7%	7,7%
Something else, what?	0,0%	0,0%	50,0%	0,0%	0,0%	50,0%
Total	**0,8%**	**20,0%**	**35,0%**	**24,6%**	**5,4%**	**14,2%**

Table 11 Significance of technology related risks to cloud security.

5.5 Protection of Cloud Services

Comprehensive security always comprises several factors, but the importance of specific security controls may be emphasized depending on the asset to be protected. Respondents were asked to assess the importance of various pre-listed security controls typically associated with cloud security. Given that the lack of security awareness and training was perceived as the most critical cloud security risk related to people, it was consequently seen as the most important people-related security control in terms of cloud security. 62% of respondents rated it as very important, while 38% rated it as important.

Security management and clearly defined roles and responsibilities related to security were both perceived as equally important, with 46% of respondents rating each as very important and another 46% rating them as important. This finding once again contrasts with the previous survey results, where 62% of respondents considered risks related to data ownership and responsibilities to be minor or moderate for cloud security Trusting the CSP was deemed either very important (31%) or important (61%) by 92% of respondents, which supports the findings of previous research. Personnel security (e.g., screening) was perceived as the most neutral security control by 15% of respondents, but over 80% still rated it as either important (62%) or very important (23%).

While 15% of respondents did not see ensuring non-disclosure obligations as very important, the majority (77%) rated it as either important (69%) or very important (8%). Ensuring and monitoring contractual obligations showed the most variation in responses; 16% did not see it as very important (8%) or rated it neutral (8%), whereas 69% rated it as important and 8% as very important. In general, people related security controls were seen as important for cloud security.

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Security management	0,0%	0,0%	0,0%	46,1%	46,2%	7,7%
Clearly defined roles and responsibilities related to security	0,0%	0,0%	0,0%	46,1%	46,2%	7,7%
Trusting the CSP	0,0%	0,0%	7,7%	61,5%	30,8%	0,0%
Ensuring and monitoring contractual obligations related to security	0,0%	7,7%	7,7%	61,5%	15,4%	7,7%
Ensuring non-disclosure obligations	0,0%	15,4%	7,7%	69,2%	7,7%	0,0%
Personnel security (e.g. screening)	0,0%	0,0%	15,4%	61,5%	23,1%	0,0%
Security awareness and training	0,0%	0,0%	0,0%	38,5%	61,5%	0,0%
Something else, what?	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Total	**0,0%**	**2,9%**	**4,8%**	**48,1%**	**28,9%**	**15,4%**

Table 12 Importance of people related security controls to cloud security.

Vulnerability management processes were deemed the most important cloud security control related to processes, with 46% of respondents stating it as very important and the remaining 54% as important. Maintaining monitoring, detection, and response capabilities was highlighted as very important by 54% of respondents and as important by 38%. Knowing the threat environment was perceived as important by 62% of respondents and very important by 38%. Incident management processes were found to be equally important and very important, each rated by 46% of respondents. Based on the survey results, it is evident that effective prevention, detection, response, and recovery procedures for various security incidents and events were generally emphasized as crucial by the respondents.

Adhering to Secure Software Development (SSDLC) principles was perceived as very important by 46% of respondents, important by 38%, and neutral by 8%. Change management processes had the highest percentage of neutral responses at 23%, but nearly 70% still saw it as important (31%) or very important (38%). Preventive business continuity management measures were found to be either important (54%) or very important (38%), with 8% viewing it as neutral. Comprehensive and up-to-date information system descriptions had the highest percentage of respondents rating it as important (69%), while 15% saw it as very important and 8% as neutral. In general, processes related security controls were mostly seen as important or very important for cloud security.

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Knowing the threat environment	0,0%	0,0%	0,0%	65,1%	38,5%	0,0%
Adhering to Secure Software Development (SSDLC) principles	0,0%	0,0%	7,7%	38,5%	46,1%	7,7%
Comprehensive and up-to-date information system descriptions	0,0%	0,0%	7,7%	69,2%	15,4%	7,7%
Change management processes	0,0%	0,0%	23,1%	30,8%	38,4%	7,7%
Maintaining monitoring, detection, and response capabilities	0,0%	0,0%	0,0%	38,5%	53,8%	7,7%
Vulnerability management processes	0,0%	0,0%	0,0%	53,8%	46,2%	0,0%
Incident management processes	0,0%	0,0%	0,0%	46,1%	46,2%	7,7%
Preventive business continuity management measures	0,0%	0,0%	7,7%	53,8%	38,5%	0,0%
Something else, what?	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Total	**0,0%**	**0,0%**	**5,1%**	**43,6%**	**35,9%**	**15,4%**

Table 13 Importance of processes related security controls to cloud security.

Cloud security controls related to technologies comprised the largest category of predefined security controls in the survey, demonstrating relatively significant variation in perceived importance among respondents. Encrypting network traffic outside the environment and identity and access management (IAM) emerged as the most critical controls, with 69% of respondents considering both to be very important and 23% viewing them as important. In contrast, encrypting network traffic within the environment was deemed very important by only 8% of respondents, important by 46%, and neutral or not very important by 23% (8% not very important).

Malware protection was also found to be a top priority, with 69% rating it as very important. Similarly, encryption key management and backup protection were both viewed as very important by 61% of respondents. However, while 31% saw backup protection as important, only 23% rated

encryption key management the same putting a little more emphasis on backup protection. The collection of log data was highlighted as critical, with 62% seeing it as very important and 38% as important. Ensuring efficient recovery processes received slightly mixed responses: 46% rated it as important, and another 46% as very important. However, it can be concluded that efficient recovery processes were seen critical for cloud security.

Other technological controls, though not as universally deemed very important, still also held significant weight. Protection of technical interfaces (e.g., API) was crucial, with 38% finding it very important and 54% important. Similarly, limiting network traffic to necessary and approved traffic was seen as very important by 31% and important by 54%. Administrative access restrictions, such as allowing access only through management portals, were also deemed as a considerable security control for cloud security, with 77% rating them as important (46%) or very important (31%). Transparency regarding data location was important to 77% of respondents, though some saw it as neutral (8%) or not very important (8%).

Segregation of the cloud environment from other environments, into separate areas, and performance and capacity management were all rated as important by 46% and very important by 23%, though opinions varied on their lesser importance. AI and machine learning in maintaining monitoring, detection, and response capabilities received varied responses, with 23% viewing them as not very important and another 23% unsure. The majority (38%) rated the use AI and machine learning as neutral in terms of cloud security.

Despite the respondents' strong technological backgrounds, physical security measures were still significant, with 38% finding them important and 31% very important, though 8% considered them less important. Federation of security among multi-clouds and application container security were similarly rated, but application container security had more divided opinions. Reliable data destruction also split opinions, with 38% viewing it as neutral, 31% as important, and 23% as very important. Overall, technology-based security controls were predominantly perceived as important or very important for maintaining cloud security.

	Not important at all	**Not very important**	**Neutral**	**Important**	**Very important**	**Unsure**
Segregation of the cloud environment from other environments	0,0%	15,4%	15,4%	46,1%	23,1%	0,0%
Segregation of the cloud environment into separate areas	0,0%	7,7%	23,1%	46,1%	23,1%	0,0%
Federation of security among multi-clouds	0,0%	0,0%	15,4%	53,8%	15,4%	15,4%

Transparency to the location of the data	0,0%	7,7%	7,7%	76,9%	0,0%	7,7%
Performance and capacity management	0,0%	0,0%	23,1%	46,1%	23,1%	7,7%
Application container security	0,0%	7,7%	7,7%	46,1%	23,1%	15,4%
Protection of technical interfaces (e.g. API)	0,0%	0,0%	0,0%	53,8%	38,5%	7,7%
Encryption key management	0,0%	0,0%	7,7%	23,1%	61,5%	7,7%
Limiting network traffic to only necessary and approved traffic	0,0%	0,0%	7,7%	53,8%	30,8%	7,7%
Encryption of network traffic within the environment	0,0%	0,7%	23,1%	46,1%	7,7%	15,4%
Encryption of network traffic outside the environment	0,0%	0,0%	0,0%	23,1%	69,2%	7,7%
Malware protection	0,0%	0,0%	23,1%	7,7%	69,2%	0,0%
Taking care of identity and access management (IAM)	0,0%	0,0%	0,0%	23,1%	69,2%	7,7%
Allowing administrative access only through certain points, such as management portal	0,0%	0,0%	23,1%	46,1%	30,8%	0,0%
Collection of log data	0,0%	0,0%	0,0%	38,5%	61,5%	0,0%
Leveraging AI and machine learning in maintaining monitoring, detection, and response capabilities	0,0%	23,1%	38,4%	7,7%	7,7%	23,1%
Protection of backups	0,0%	0,0%	7,7%	30,8%	61,5%	0,0%
Reliable destruction of data	0,0%	0,0%	38,4%	30,8%	23,1%	7,7%
Ensuring efficient	0,0%	0,0%	7,7%	46,1%	46,2%	0,0%

recovery processes						
Physical security measures	0,0%	7,7%	15,4%	38,4%	38,8%	7,7%
Something else, what?	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Total	**0,0%**	**3,7%**	**13,6%**	**37,3%**	**34,1%**	**11,4%**

Table 14 Importance of technology related security controls to cloud security.

6 DISCUSSION

Cloud computing offers numerous benefits for organizations and adoption of cloud solutions can also bring significant improvements for the security of information systems, which would potentially be otherwise out of the organization's reach. However, cloud solutions are also complex environments that include various layers, components, and actors – all with their own purposes and weaknesses. To efficiently protect the cloud environments, it is critical that all actors understand the risks they are facing and mitigate them accordingly.

The organization's understanding of cloud-specific attributes, architectural components for each cloud service and deployment model, and the exact role of each cloud actor in cloud security, is crucial for the successful adoption of the cloud (Luna et al., 2015). Khalil et al. (2014) proposed that addressing cloud security issues comprehensively begins with a thorough understanding of the various security attributes inherent in cloud environments and their implications across different deployment and service models. It involves identifying the specific security requirements relevant to the organization, as well as identifying the parties and stakeholders involved, along with their respective roles and responsibilities in ensuring cloud security (Khalil et al., 2014).

Before adopting cloud solutions, organizations should conduct a thorough review of their processes and assess the risks and opportunities associated with adopting cloud solutions, and what value does it bring to the organization (Avram, 2014; Zhu et al., 2012). Not all cloud deployment or service models are universally suitable for every purpose, and the security levels among different CSPs and cloud solutions can vary significantly (Butt et al., 2022). For example, public clouds are generally perceived as more vulnerable compared to for instance private clouds, as public cloud is based on the principle that anyone can use or host services in that environment, including potentially malicious users (Morsy et al., 2016; Subashini & Kavitha, 2010). This process can be time-consuming and exhaustive, particularly for large organizations with various complex processes, but still necessary as even if the responsibilities

regarding cloud security can be shared with the CSP and other involved parties, the accountability remains within the organization (Avram, 2014; Jansen, 2011). While there are no universal or standardized SLA models for cloud services suitable for all needs, organizations need to carefully consider the contractual requirements between themselves and the CSP (Jansen, 2011). To enhance automation and usability, it is recommended to design a standardized cloud SLA template for the organization, which can serve as a basis when adopting new cloud solutions (Luna et al., 2015). The SLA should include necessary elements related to the security of the cloud solution, such as security policies and frameworks to adhere to, required security controls and their implementation, related roles and responsibilities, and possible sanctions if the SLA is not followed (Kandukuri et al., 2009; Luna et al., 2015). Designing a separate security service level agreement (secSLA) in addition to the general cloud SLA or master service agreement can be particularly useful and clarifying for complex or large entities (Luna et al., 2015).

Organizations can leverage several well-known cloud security frameworks to implement best practices, such as the NIST Cloud Security Framework, CSA STAR, ISO/IEC 27017, COBIT 5, and the AWS Well-Architected Framework (Chauhan & Shiaeles, 2023). Particularly, the latter was emphasized by the survey respondents for this study, along with ISO/IEC 27001 which was also highlighted by Di Giulio et al. (2017) to show good performance in terms of protecting cloud assets. Although ISO/IEC 27001 does not solely focus on cloud security but on creating and maintaining an information management system in general, it also emphasizes important security controls relevant to cloud security, such as robust asset management and change control processes (Torkura et al., 2021). These frameworks provide organizations valuable guidelines and controls to protect cloud environments against both external and internal threats, and mitigating common risks associated with cloud environments (Chauhan & Shiaeles, 2023). However, each framework has its own characteristics, strengths, and weaknesses (Chauhan & Shiaeles, 2023). There is no single framework that serves as a silver bullet to effectively address security concerns for every cloud environment (Chauhan & Shiaeles, 2023; Di Giulio et al., 2017). Therefore, organizations should carefully evaluate and choose the framework or combination of frameworks that best suits their specific needs (Chauhan & Shiaeles, 2023).

Leveraging industry best practices and innovative technologies such as AI and machine learning together with current security solutions such as SIEM and IDS can be helpful in effectively mitigating the risks associated with cloud security (Carrera, 2022; Gururaj et al., 2017; Subramanian & Tamilselvan, 2019). Data breaches, unauthorized access, insecure APIs, insider risks, and insufficient security measures are some examples among the major security concerns for organizations using cloud solutions. However, these issues can be effectively managed with proactive and robust security controls (Chauhan & Shiaeles, 2023).

Organizations should ensure that the security measures protecting the physical layer of the cloud infrastructure are implemented sufficiently, and effective disaster recovery controls are in place to mitigate any potential damage to the physical layer, whether caused naturally or intentionally (Subashini & Kavitha, 2010). Indeed, the cloud infrastructure's underlying infrastructure layer encompassing the cloud's physical infrastructure, network and virtualization layer, can be considered the most critical in terms of cloud security. Since all other layers reside on top of it, any weakness or vulnerability in this layer will affect the layers above it (Morsy et al., 2016).

For a long time, this so-called IaaS layer was considered the most vulnerable and prone to various security issues (Subashini & Kavitha, 2010). However, over the years, CSPs have significantly improved the security level of this layer and security issues or attacks against the underlying infrastructure are no longer that common (Torkura et al., 2021). Conversely, the upper layers of the cloud infrastructure, where customers are responsible for security, have become more vulnerable to attacks, largely due to misconfigurations and human errors (Torkura et al., 2021). This highlights the importance of cloud security controls that address human errors, such as clearly defining and communicating roles and responsibilities related to cloud security, raising awareness about security risks associated with cloud solutions, and educating users on how to avoid or mitigate these risks (Chauhan & Shiaeles, 2023; Torkura et al., 2021).

Just like security issues exist at all layers of cloud environments, they also exist throughout all stages of the data lifecycle (Deyan & Hong, 2012). When considering the protection of data residing in the cloud, it's important for organizations to recognize that data remains data, irrespective of its storage location, handling, or transmission method. Hence, the fundamental principles of safeguarding data throughout its lifecycle remain applicable in the cloud context as well, and organizations should ensure that their data is protected according to their policies, whether they are utilizing cloud solutions or not (Jansen, 2011; Xiaojun & Qiaoyan, 2010).

While cloud solutions are frequently compared to traditional IT systems, they share the same basic components and technologies (Subashini & Kavitha, 2010). Since cloud services are constructed over the internet, they also inherit all the security concerns associated with internet-based environments, and to secure data transmission within the cloud and to and from the cloud, similar principles apply as those used to protect data traffic over the internet, such as implementing robust encryption policies and secure protocols (Subashini & Kavitha, 2010). Network level security risks and mitigation measures have been studied and applied long before the advent of cloud computing, rendering these security controls highly mature and effective, but just like with any devices or services connected to the internet, it's crucial to prioritize protecting cloud environments from external network attacks (Coppolino et al., 2017). This

involves implementing robust security controls to ensure the environment is secure, private, and isolated (Subashini & Kavitha, 2010).

While cloud computing shares foundational principles and components with traditional IT systems and addresses many vulnerabilities effectively, its dynamic nature can challenge the efficacy of traditional countermeasures (Zissis & Lekkas, 2012). The numerous challenges associated with cloud security underscore the critical need for organizations to implement robust security controls, conduct comprehensive risk assessments, and ensure continuous monitoring and development of their cloud environments (Chauhan & Shiaeles, 2023). Implementing security controls that support each other such as strict IAM policies and access control restrictions, encrypting sensitive data, conducting regular security assessments, and utilizing effective authentication controls like MFA can effectively address these concerns. Consequently, efficient security management is crucial for controlling and managing the various required security mechanisms, which should be dynamic and autonomous by nature, and consistently applied across the entire cloud environment and its supporting structures, particularly when developing or adopting new systems, processes, services, or applications (Duncan, 2020; Khalil et al., 2014; Morsy et al., 2016). The selection of security controls should be in balance with the risks involved, as implementing an excessive number or overly stringent controls can also prove to be ineffective and inefficient (Jansen, 2011).

Since cloud environments are rarely static but rather constantly evolving with new technologies while new workloads and capabilities are added according with current needs, it is essential to remain adaptive and commit to continuous improvement to ensure that cloud security develops alongside with the cloud environment and the surrounding threat landscape (Duncan, 2020; Khalil et al., 2014; Morsy et al., 2016). Even if the cloud solution itself would stay the same, the threat landscape is still constantly changing (Duncan, 2020). Organizations should take a holistic and multilayered security approach for cloud security adhering to the defense in depth principles, ensuring that security is integrated into every layer of the cloud environment by design, meaning that security is rather built into the cloud architecture from the start than added later (Casola et al., 2016; Chang et al., 2016; Deyan & Hong, 2012; Duncan, 2020; Gururaj et al., 2017; Khalil et al., 2014).

7 CONCLUSION

The objective for this thesis was to improve awareness among organizations regarding the security risks associated with cloud computing and the methods and tools available to mitigate these risks. This was achieved through by examining the security risks inherent in cloud computing and determining how and why organizations should address these risks when adopting or using cloud services. The study aimed to answer one main research question: *"What should organizations take into account regarding information security when deploying and managing cloud services?"*, and one sub-research question: *"What information security risks can the use of cloud services cause for organizations?"*. The structure of the thesis encompassed a thorough literature review covering chapters 2-3, followed by an empirical case study covering chapters 4-6.

The theoretical foundation for the study was established through the literature review presented in chapters 2-3. The second chapter first introduced the definition of cloud computing and cloud services, described the actors involved, and explored the service delivery and deployment models used in cloud computing. Towards the end of the second chapter, the basic elements of cloud architecture were identified and explained, followed by a concise overview of the advantages organizations can gain through the adoption of cloud solutions. The third chapter described the typical risks associated with cloud security from the organizations' perspective and the potential security measures than can be employed to mitigate these risks. The empirical section of the thesis was presented in chapters 4-6. The fourth chapter, focused on the research methods used in the study, their implementation, and the process of data collection while using a survey as a method. The fifth chapter presented the survey results and their analysis. The study's findings were discussed in the sixth chapter, finally followed by a conclusion of the thesis in this seventh chapter.

Cloud computing presents numerous advantages for organizations, yet it also introduces various risks and vulnerabilities. Effectively safeguarding cloud environments requires organizations to comprehensively understand these risks and take appropriate measures to mitigate them. This involves gaining a

deep understanding of cloud-specific characteristics, architectural components specific to each cloud service and deployment model, and the specific roles of different entities in ensuring cloud security. Before adopting cloud solutions, organizations should conduct a thorough assessment of their existing processes and evaluate the associated risks and benefits. It's crucial to determine how adopting cloud solutions aligns with organizational objectives and the value it brings. Leveraging well-known security frameworks such as ISO/IEC 27001 can provide organizations with essential guidelines and controls to implement industry best practices for protecting cloud environments. These frameworks offer valuable insights and recommendations to enhance cloud security posture effectively.

The numerous challenges associated with cloud security highlight the critical need for organizations to implement robust security controls, conduct comprehensive risk assessments, and ensure continuous monitoring and development of their cloud environments. It is essential for organizations to remain adaptive and commit to continuous improvement to ensure that cloud security evolves alongside the cloud environment and the surrounding threat landscape. Organizations should adopt a comprehensive and multilayered approach to cloud security, adhering to the defense-in-depth principles. This includes ensuring that security is integrated into every layer of the cloud architecture by design.

REFERENCES

Alassafi, M.O., Alharthi, A., Walters, R.J. & Wills, G.B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics, 34*, 996-1010.

Albladi, S.M. & Weir, G.R.S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity, 3(7)*, 1-19.

Almorsy, M., Grundy, J. & Ibrahim, A.S. (2011). Collaboration-Based Cloud Computing Security Management Framework. *IEEE 4th International Conference on Cloud Computing* (pp. 364-371). Washington, DC, USA.

Amazon Web Services. (9.5.2024a). *Shared Responsibility Model.* https://aws.amazon.com/compliance/shared-responsibility-model/

Amazon Web Services. (7.5.2024b). *What is a hypervisor?.* https://aws.amazon.com/what-is/hypervisor/

Amazon Web Services. (11.5.2024c). *What's the Difference Between SSL and TLS?.* https://aws.amazon.com/compare/the-difference-between-ssl-and-tls/

Arachchilage, N.A.G., Love, S. & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197.

Arora, A., Khanna, A., Anmol, R. & Agarwal, A. (2017). Cloud Security Ecosystem for Data Security and Privacy. *7th International Conference on Cloud Computing, Data Science & Engineering* (pp. 288-292). Noida, India.

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology, Vol. 12*, 529-534.

Beckers, K., Côté, I., Faßbender, S., Heisel, M. & Hofbauer, S. (2013). A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance. *Requirements Engineering for Security, Privacy & Services in Cloud Environments, 18*, 343-395.

Bohn, R.B., Messina, J., Liu, F., Tong, J. & Mao, J. (2011). NIST Cloud Computing Reference Architecture. *2011 IEEE World Congress on Services* (pp. 594-596). Washington, DC, USA.

Broadcom. (7.5.2024a). *What is a hypervisor?*. https://www.vmware.com/topics/glossary/content/hypervisor.html

Broadcom. (7.5.2024b). *What is a virtual machine?*. https://www.vmware.com/topics/glossary/content/virtual-machine.html

Bullée, J-W.H., Montoya, L., Pieters, W., Junger, M. & Hartel, P. (2018). On the anatomy of social engineering attacks – A literature-based dissection of successful attacks. *J Investig Psychol Offender Profil*, *15*, 20-45.

Butt, U.A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M.T. & Albaqami, N. (2022). Cloud Security Threats and Solution: A Survey. *Wireless Personal Communications, 128*, 387-413.

Carrera, G. (2022). Building a comprehensive cloud security audit program. *EDPACS, 66*(1), 15-19.

Casola, V., De Benedicts, A., Rak, M. & Rios, E. (2016). Security-by-design in clouds: a Security-SLA driven methodology to build secure cloud applications. *Procedia Computer Science, 97*, 53-62.

Chang, V., Kuo, Y.-H. & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems, 57*, 24-41.

Chauhan, M. & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network, 3*(3), 422–450.

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering, 59*, 126-140.

Deyan, C. & Hong, Z. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *International Conference on Computer Science and Electronics Engineering* (pp. 647-651). Hangzhou, China.

Di Giulio, C., Kamhoua, C., Campbell, R.H., Sprabery, R., Kwiat, K. & Bashir, M.N. (2017). Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security. *IEEE 10th International Conference on Cloud Computing* (pp. 50-57). Honolulu, HI, USA.

Duncan, R. (2020). A multi-cloud world requires a multi-cloud security approach. *Computer Fraud & Security, 5*, 11-12.

Ebot, A.T (2018). Using stage theorizing to make anti-phishing recommendations more effective. *Information & Computer Security*, *26(4)*, 401-419.

Esposito, C. & Castiglione, A. (2016). Cloud Manufacturing: Security, Privacy, and Forensic Concerns. *IEEE cloud computing, 3*(4), 16–22.

Google. (9.5.2024). *Shared responsibilities and shared fate on Google Cloud.* https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Gupta, B.B., Tewari, A., Jain, A.K. & Agrawal, D.P. (2016). Fighting against phishing attacks: state of art and future challenges. *Neural Comput & Applic, 28*, 3629-3654.

Gupta, B.B., Arachchilage, N.A.G., & Psannis, K.E. (2017). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommun Syst., 67*, 247-267.

Gururaj, R., Mohsin, I. & Farrukh, A. (2017). A Comprehensive Survey on Security in Cloud Computing. *Procedia Computer Science, 110*, 465-472.

Jansen, W. A. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. *Proceedings of the 44th Hawaii International Conference on System Sciences* (pp. 1-10). Kauai, HI, USA.

Kalaiprasath, R., Elankavi, R. & Udayakumar, R. (2017). Cloud Security and Compliance – A Semantic Approach in End to End Security. *International Journal on Smart Sensing and Intelligent Systems Special Issue, 10*(5), 482-494.

Kandukuri, B.R., Paturi, V.R. & Rakshit, A. (2009). Cloud Security Issues. *IEEE International Conference on Services Computing* (pp. 517-520). Bangalore, India.

Khalil, I.M., Khreishah, A. & Azeem, M. (2014). Cloud Computing Security: A Survey. *Computers, 3*, 1-35.

Khan, N. & Al-Yasiri, A. (2016). Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. *Procedia Computer Science, 94*, 485-490.

Lance, J., & Jevans, D. (2005). Phishing Exposed. *Elsevier Science & Technology Books.*

Lastdrager, E.E.H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3(9)*, 1-10.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. & Leaf, D. (2011). *NIST Cloud Computing Reference Architechture*. National Institute of Standards and Technology. https://www.nist.gov/publications/nist-cloud-computing-reference-architecture

Luna, J., Suri, N., Iorga, M. & Karmel, A. (2015). Leveraging the Potential of Cloud Security Service-Level Agreements through Standards. *IEEE cloud computing, 2*(3), 32-40.

Mandal, S. & Khan, D.A. (2021). Comprehensive Survey of Security Issues & Framework in Data-Centric Cloud Applications. *Journal of Engineering Science and Technology Review, 14*(1), 1-24.

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/145/final

Microsoft. (9.5.2024a). *Shared responsibility in the cloud.* https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Microsoft. (7.5.2024b). *Virtual Machines: virtual computers within computers.* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine

Morsy, M., Grundy, J. & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. *Ithaca*, 1-6.

Myers, M. (2020). *Qualitative research in business & management (3rd edition).* SAGE Publications Ltd.

Naone, E. (2009). *Conjuring Clouds: How engineers are making on-demand computing reality*. MIT Technology Review. https://www.technologyreview.com/2009/06/23/212416/conjuring-clouds/

OpenAI. (16.6.2024). *ChatGPT.* https://chatgpt.com/

OWASP. (12.5.2024a). *OWASP Top 10 API Security Risks - 2023.* https://owasp.org/API-Security/editions/2023/en/0x11-t10/

OWASP. (13.5.2024b). *OWASP Top 10.* https://owasp.org/www-project-top-ten/

Qazi, F.A. (2023). Application Programming Interface (API) Security in Cloud Applications. *EAI endorsed transactions on cloud systems, 7*(23), 1-14.

Rao R.R. & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science, 48*, 204–209.

Rebollo, O., Mellado, D., Fernández-Medina, E. & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57.

Red Hat. (12.5.2024). *What does an API gateway do?.* https://www.redhat.com/en/topics/api/what-does-an-api-gateway-do

Rizvi, S., Ryoo, J., Kissel, J., Aiken, W. & Liu, Y. (2017). A security evaluation framework for cloud security auditing. *The Journal of Supercomputing, 74*, 5774-5796.

Salminen, S. (2011). *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin* (Opetusjulkaisuja 62). Vaasan Yliopisto. http://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Schaab, P., Beckers, K. & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information & Computer Security*, *25(2)*, 206-222.

Siddiqi, M.A., Pak, W., & Siddiqi, M.A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Appl. Sci.*, *12*, 1-19.

Singh, A. & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, 79*, 88–115.

Singh, S., Jeong, Y.-S. & Park, J.H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications, 75*, 200-222.

Sisodia, J. & Khan, M (2022). *The Customer's Responsibility in the Cloud: Shared Responsibility Model*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-customers-responsibility-in-the-cloud-shared-responsibility-model

Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N. & Lo lacono, L. (2011). All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces. *In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, 11* (pp. 3-14). NY, USA.

Soms, N., Oswalt, M.S. & Santhos, K.P. (2022). A case study on cloud security controls. *International Journal of Health Sciences, 6*(S1), 11374-11380.

Stanoevska-Slabeva, K., Wozniak, T. & Ristol, S. (2010). *Grid and Cloud Computing: A Business Perspective on Technology and Applications*. Springer.

Subashini, S. & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*, 1–11.

Subramanian, E.K. & Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security. *Service Oriented Computing and Applications, 13*, 237-249.

Sun, X. (2018). Critical Security Issues in Cloud Computing: A Survey. *IEEE 4th International Conference on Big Data Security on Cloud* (pp. 216-221). Omaha, NE, USA.

Sur, C. (2018). Ensemble one-vs-all learning technique with emphatic & rehearsal training for phishing email classification using psychology. *Journal of Experimental & Theoretical Artificial Intelligence, 30(6),* 733-762

Torkura, K.A., Sukmana, M.I.H., Cheng, F. & Meinel, C. (2021). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security, 102*, 102-124.

Walterbusch, A., Fietz, A. & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. *Journal of Enterprise Information Management, 30*(4), 644-665.

Wang, Z., Zhu, H. & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access, 13*, 11895-11910

Wright, D., Smith, D., Ji, K., Borrega, M.A., Galimberti, A. & Bauman, S. (2023). *Magic Quadrant for Strategic Cloud Platform Services*. Gartner, inc. https://www.gartner.com/doc/reprints?id=1-2ES4ML14&ct=230823

Wright, R.T. & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27(1)*, 273-303.

Xiaojun, Y. & Qiaoyan, W. (2010). A View about Cloud Data Security from Data Life Cycle. *International Conference on Computational Intelligence and Software Engineering* (pp. 1–4). Wuhan, China.

Zhu, Y., Liu, P. & Wang, J. (2012). Cloud security research in Cloud Computing. *Applied Mechanics and Materials, 198-199*, 415-419.

Zissis, D. & Lekkas, L. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*, 583–592.

APPENDIX 1: SURVEY TEMPLATE

Information Security and Risk Management of Cloud Services

Dear Study Participant,

Thank you for participating in the survey of my master's thesis. Answering the survey takes approximately 20 minutes. The given answers are treated as confidential and the information of persons or organizations will not be published nor disclosed to 3rd parties. In the thesis, sources are referred as: Participant1, Participant2, Organization1, Organization2..etc. If you wish, you can also participate anonymously, or leave the name of your organization blank.

If you wish, you can also participate in a lottery, where 2 Apple Gift Cards worth 25 euros will be drawn among all participants.

Background
Cloud services are widely used by companies, educational institutions, and individuals, and the increase in their use so far shows little sign of slowing down. As the use of cloud services increases, the security of the solutions is also more often the subject of scrutiny in organizations, and some organizations even postpone the adoption of cloud services or the expansion of their use due to security concerns or a lack of expertise and understanding.

In the midst of the flood of information and offers related to cloud security solutions, it can be difficult for organizations to understand what should be treated as essential, which information security controls should they focus on, and which guidelines or frameworks to rely on. From an organizational perspective, the problem can be considered to be multidimensional, and among other things, it is concretized in the form of shortage of talent, lack of maturity, conflicting best practices and frameworks, and complex commercial structures of the service providers and suppliers.

Subject of the study
The baseline of the research are organizations that use or produce cloud solutions. The aim of the research is to determine how and why organizations should address information security when adopting or using cloud services. One main research question has been defined for the thesis, and two sub-research questions to support this, which the study aims to answer:

- What should organizations take into account regarding information security when deploying and managing cloud services?
    - What information security risks can the use of cloud services cause for organizations?
    - What information security standards and frameworks can organizations use when evaluating or developing the security of their cloud services?

Author
I am a fifth-year cyber security master's student at the University of Jyväskylä, specializing in overall security and strategic intelligence. I have worked in different types of corporate security positions for about 20 years, of which the last 5 years have been mainly focused on the area of information security. The results of the thesis, which will be completed later in the summer of 2024, will be distributed to each participant, if the participant so wishes.

Respectfully,
Tommi Törmänen

Participant

1. Participant information

If you wish, you can also participate anonymously. The names or titles of the participants will not be published or disclosed to 3rd parties. In the thesis, sources are referred as: Participant1, Participant2..etc.

Name

Title

Country *

2. Experience

How long have you worked in your current position and in the service of your current employer? State your answer in even years.

Current position *

Current organization *

3. Job description/ areas of responsibility *

Briefly describe what your job description includes/ what your main areas of responsibility are, and how cloud solutions are reflected in your current duties. Are you a user of cloud solutions, do you sell them, do you work in the design, development, or maintenance of cloud services, or do you govern security issues related to them for example?

Participants background organization

4. Information of the background organization

If you wish, you can leave the name of your organization blank. The names of the organizations will not be published or disclosed to 3rd parties. The number of personnel can be reported as an estimate.

Name

Industry *

Number of personnel *

5. Operating sector *

Does your organization operate in the:

- ◯ Private sector
- ◯ Public sector

6. Use of cloud services *

Does your organization use cloud services?

- ◯ Yes
- ◯ No
- ◯ Unsure

7. Used cloud service models

Which of the following cloud service models does your organization use?

	Yes	No	Unsure
Infrastructure as a Service (IaaS) *	◯	◯	◯
Platform as a Service (PaaS) *	◯	◯	◯
Software as a Service (SaaS) *	◯	◯	◯
Something else, what?	◯	◯	◯

9. Cloud Service Provider *

Does your organization provide cloud services?

- ◯ Yes
- ◯ No
- ◯ Unsure

10. Provided cloud service models

Which of the following cloud service models does your organization provide?

	Yes	No	Unsure
Infrastructure as a Service (IaaS) *	◯	◯	◯
Platform as a Service (PaaS) *	◯	◯	◯
Software as a Service (SaaS) *	◯	◯	◯
Something else, what? _____	◯	◯	◯

11. Provided cloud models

Which of the following cloud models does your organization provide?

	Yes	No	Unsure
Private Cloud *	◯	◯	◯
Public Cloud *	◯	◯	◯
Hybrid Cloud *	◯	◯	◯
Something else, what? _____	◯	◯	◯

Benefits of cloud services

12. Attitude towards cloud services *

How would you describe the attitude towards cloud services in your organization?

	1	2	3	4	5	
Very cautious	○	○	○	○	○	Very open

13. The impact of risk management and security on attitudes towards cloud services *

How strongly would you rate this attitude to be affected by concerns of the risks or security issues related to cloud services?

	1	2	3	4	5	
No effect	○	○	○	○	○	Significant effect

14. Benefits of cloud services

Listed below are the benefits generally associated with the adoption of cloud services compared to traditional information systems. How would you rate the importance of these benefits for your own organization when making an assessment of the transition to using a cloud solution?

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Cost-efficiency *	○	○	○	○	○	○
Rapid deployment *	○	○	○	○	○	○

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Scalability *	○	○	○	○	○	○
Data shareability *	○	○	○	○	○	○
Accessibility of services *	○	○	○	○	○	○
Interoperability of systems *	○	○	○	○	○	○
Operational reliability and continuity *	○	○	○	○	○	○
Something else, what?	○	○	○	○	○	○

15. Benefits of cloud services in risk management and security

Briefly describe the most important benefits in terms of risk management and security that you think it is possible to achieve by adopting cloud services?

Cloud Service Providers

16. Choosing a cloud service provider

What should be considered in terms of risk management and security when choosing a cloud service provider? What are the most important factors that can be used to ensure the reliability of a cloud service provider?

17. Contracts

How should risk management and security be taken into account in contracts with cloud service providers?

Security of cloud solutions

18. Security level of cloud services *

At what level do you feel the security of the cloud services used by your organization is in general?

Very bad	Bad	Average	Good	Very good	Unsure
○	○	○	○	○	○

19. Influencing the level of security *

Do you feel that you can influence the level of security of the cloud services in use?

Completely disagree	Disagree	Neither agree or disagree	Agree	Completely agree	Unsure
○	○	○	○	○	○

20. Critical data and services *

Has your organization moved critical data or services to the cloud?

- ○ Yes
- ○ Partly
- ○ No
- ○ Unsure

21. Restriction or prohibition of use *

Has your organization not adopted or limited the use of some cloud solutions due to security concerns?

- ○ Yes
- ○ Partly
- ○ No
- ○ Unsure

Cloud security risks

Listed below are information security-related risk factors typically associated with cloud solutions, which have been roughly grouped into three different categories; people, process and technology-related risks. How big do you personally perceive these risk factors to be in terms of cloud security?

22. Risks, People

	Insignificant	Minor	Moderate	Significant	Critical	Unsure
Insider risks (malicious) *	○	○	○	○	○	○
Lack of security awareness or training *	○	○	○	○	○	○
Data Leak/ Data Loss *	○	○	○	○	○	○
Unauthorized cloud resource abuse (e.g. mining crypto, executing DOS attacks etc.) *	○	○	○	○	○	○
Something else, what? _____	○	○	○	○	○	○

23. Risks, Processes

	Insignificant	Minor	Moderate	Significant	Critical	Unsure
Organization's business models do not support cloud solutions *	○	○	○	○	○	○
Compliance risks (laws and regulations) *	○	○	○	○	○	○
Risks arising from inadequate contract models in terms of security *	○	○	○	○	○	○
Risks related to data ownership and responsibilities *	○	○	○	○	○	○
Risks related to limited visibility (location of data, security controls) *	○	○	○	○	○	○
Identity and access management risks (IAM) *	○	○	○	○	○	○
Risks related to encryption key management *	○	○	○	○	○	○
Risks related to backup protection *	○	○	○	○	○	○
Risks related to data destruction and retention processes *	○	○	○	○	○	○
Something else, what? _____	○	○	○	○	○	○

24. Risks, Techonologies

	Insignificant	Minor	Moderate	Significant	Critical	Unsure
Risks arising from vulnerabilities in shared technology *	○	○	○	○	○	○
Risks related to system architecture *	○	○	○	○	○	○
Risks related to virtualization vulnerabilities *	○	○	○	○	○	○
Risks related to web application vulnerabilities *	○	○	○	○	○	○
Risks related to technical interfaces (e.g. API) *	○	○	○	○	○	○
Service availability issues *	○	○	○	○	○	○
Compatibility issues between cloud platforms *	○	○	○	○	○	○
Account, Service, and Traffic High-Jacking *	○	○	○	○	○	○
Denial of service attacks *	○	○	○	○	○	○
Something else, what?	○	○	○	○	○	○

25. Knowledge of security risks *

How well would you rate your organization is aware of security risks related to cloud solutions?

Poorly	Not very well	Moderately	Well	Very well	Unsure
○	○	○	○	○	○

Protection of cloud services

Overall security always consists of the sum of several factors, but the importance of certain controls may be emphasized depending on the asset to be protected. How important do you think the following controls are in terms cloud security?

26. Controls, People

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Security Management *	○	○	○	○	○	○
Clearly defined roles and responsibilities related to security *	○	○	○	○	○	○
Trusting the cloud service provider *	○	○	○	○	○	○
Ensuring and monitoring contractual obligations related to security *	○	○	○	○	○	○
Ensuring non-disclosure obligations *	○	○	○	○	○	○

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Personnel security (e.g. screening) *	○	○	○	○	○	○
Security awareness and training *	○	○	○	○	○	○
Something else, what? _____	○	○	○	○	○	○

27. Controls, Processes

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Knowing the threat environment *	○	○	○	○	○	○
Adhering of Secure Software Development (SSDLC) principles *	○	○	○	○	○	○
Comprehensive and up-to-date information system descriptions *	○	○	○	○	○	○
Change management processes *	○	○	○	○	○	○
Maintaining monitoring, detection, and response capabilities *	○	○	○	○	○	○
Vulnerability management processes * *	○	○	○	○	○	○
Incident management processes *	○	○	○	○	○	○
Preventive business continuity management measures *	○	○	○	○	○	○
Something else, what? _____	○	○	○	○	○	○

28. Controls, Technologies

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Segregation of the cloud environment from other environments *	○	○	○	○	○	○
Segregation of the cloud environment into separate areas *	○	○	○	○	○	○
Federation of security among multi-clouds *	○	○	○	○	○	○
Transparency to the location of the data *	○	○	○	○	○	○
Performance and capacity management *	○	○	○	○	○	○
Application container security *	○	○	○	○	○	○
Protection of technical interfaces (e.g. API) *	○	○	○	○	○	○

	Not important at all	Not very important	Neutral	Important	Very important	Unsure
Encryption key management *	○	○	○	○	○	○
Limiting network traffic to only necessary and approved traffic *	○	○	○	○	○	○
Encryption of network traffic within the environment *	○	○	○	○	○	○
Encryption of network traffic outside the environment *	○	○	○	○	○	○
Malware protection *	○	○	○	○	○	○
Taking care of identity and access management (IAM) *	○	○	○	○	○	○
Allowing administrative access only through certain points, such as management portal *	○	○	○	○	○	○
Collection of log data *	○	○	○	○	○	○
Leveraging AI and machine learning in maintaining monitoring, detection, and response capabilities *	○	○	○	○	○	○
Protection of backups *	○	○	○	○	○	○
Reliable destruction of data *	○	○	○	○	○	○
Ensuring efficient recovery processes *	○	○	○	○	○	○
Physical security measures *	○	○	○	○	○	○
Something else, what?	○	○	○	○	○	○

29. Main areas of development

Which controls do you see as the most important development areas for your own organization?

30. Standards and frameworks

Does your organization use any of the following standards, frameworks, and tools for evaluating and developing the security of cloud solutions?

- [ ] AWS Well-Architected Framework
- [ ] CIS Controls Cloud Companion Guide
- [ ] CCM (Cloud Controls Matrix)
- [ ] CMMC (Cybersecurity Maturity Model Certification)
- [ ] COBIT 5
- [ ] CSA Security Guidance
- [ ] CSA STAR (Security, Trust, Assurance, and Risk program)
- [ ] ENISA Cloud Computing Risk Assessment
- [ ] ENISA Cloud Security Guide
- [ ] FedRAMP (Federal Risk and Authorization Management Program)
- [ ] ISO 27001/ ISO 27002 (Information security management systems/ controls)
- [ ] ISO 27017 (Information security controls for cloud services)
- [ ] ISO 27018 (Protection of personally identifiable information (PII) in public clouds acting as PII processors)
- [ ] Katakri (NSA Finland, Information security auditing tool for authorities)
- [ ] NIST SP800-53 (Security and Privacy Controls for Information Systems and Organizations)
- [ ] NIST SP800-144 (Guidelines on Security and Privacy in Public Cloud Computing)
- [ ] OWASP Top Ten
- [ ] PiTuKri (Traficom, Criteria for Assessing the Information Security of Cloud Services)
- [ ] SOC 2 (Systems and Organizations Controls 2)
- [ ] Someting else, what?
- [ ] Unsure

31. Advantages and disadvantages of the standards and frameworks used

Briefly describe the advantages and disadvantages of the standards and frameworks used in terms of evaluating and developing cloud security. If multiple standards and frameworks are used, you can describe the advantages and disadvantages of only the most important ones.

32. Audits *

Is the security of your cloud solutions audited regularly?

- [ ] Yes, External audits
- [ ] Yes, Internal audits
- [ ] No
- [ ] Unsure

33. Certifications or approvals required

Do you require security-related certificates or approvals from your cloud service providers in your organization? What?

34. The benefits of standards and frameworks

Briefly describe what is your opinion about the standards and frameworks related to cloud security?

Thank you for participating in the survey of my master's thesis!

35. Sharing the results of the thesis and participating in the lottery

☐ I would like the results of the thesis to be shared with me after it is completed.

☐ I would like to take part in the Apple Gift Card draw.

36. Email address to which I want the results of the thesis to be shared:

The email address provided will not be used for any other purpose, such as direct marketing or commercial purposes.

E-mail

37. Email address to which I want the Apple Gift Card to be delivered if I win the draw:

The e-mail address provided will not be used for any other purpose, such as direct marketing or commercial purposes.

E-mail

Lottery instructions and rules

- 2 Apple Gift Cards worth 25 euros will be drawn among all survey participants.
- The lottery participation period ends on April 14, 2024.
- The draw will take place on April 15, 2024, and the winners will be contacted at the given email address.
- All persons of legal age can participate in the draw.
- The University of Jyväskylä is not participating in the lottery.
- Participating in the lottery requires providing an email address.

38. Casual remarks

Is there anything else you would like to add or comment before the end of the survey?