Recent challenges and solutions in cloud data security

A literature review

Bachelor's Thesis
Degree Programme in Business Information Technology
Autumn 2025
Saga Payling-Nyhuus

HAMK
Häme University
of Applied Sciences

HAMK
Hämeen ammatti-
korkeakoulu

Tiivistelmä

Koulutus	Tietojenkäsittelyn koulutus	
Tekijä	Saga Payling-Nyhuus	Vuosi 2025
Työn nimi	Recent challenges and solutions in cloud data security	
Ohjaajat	Ismo Turve ja Lasse Seppänen	

Tämän ammattikorkeakoulun opinnäytetyön tavoitteena oli tarkastella pilvidatan tietoturvan nykytilaa erityisesti pilvipalveluiden asiakkaan näkökulmasta. Opinnäytetyön tutkimuskysymykset olivat seuraavat: (1) Mitkä ovat pilvidatan tietoturvan keskeiset käsitteet ja miten pilvitietoturvaa hallitaan? (2) Mitkä ovat tärkeimmät haasteet pilvidatan tietoturvassa nykykirjallisuuden mukaan? (3) Mitä uusia teknologisia ratkaisuja on esitelty pilvidatan tietoturvan parantamiseksi aikavälillä 1/2024–2/2025, ja mitä haasteita ne pyrkivät ratkaisemaan?. Työ ei perustu toimeksiantoon, vaan sen taustalla oli havaittu vähäisyys ajantasaisissa kirjallisuuskatsauksissa aiheesta sekä tekijän ammatillinen kiinnostus pilvidatan tietoturvaa kohtaan.

Kyseessä on teoreettinen tutkimus, joka pohjautuu olemassa olevaan kirjallisuuteen. Teoreettinen viitekehys rakentuu luvuista 2-6. Luvuissa 2-5 käsitellään muun muassa pilvipalveluiden palvelu- ja käyttöönottomalleja (service and deployment models), sekä jaetun vastuun mallia (shared responsibility model). Lisäksi esitellään tietoturvan elinkaarta (secure data lifecycle), CIA-kolmiota (confidentiality, integrity, availability), sekä EU:n tietosuoja-asetusta (General Data Protection Regulation). Luvuissa tarkastellaan myös keskeisiä pilvidatan tietoturvaratkaisuja, sekä alan suosituksia Cloud Security Alliance (CSA) -organisaation ja Microsoftin Cloud Security Benchmark -viitekehysten pohjalta. Luku 6 käsittelee tietoturvahaasteita nykyaikaisissa pilviympäristöissä, kuten pääsynhallinnan (access control) epäselvyyksiä, valvontajärjestelmien (monitoring systems) puutteita sekä erilaisia haasteita datan suojaamisessa. Tarkastelu perustuu ajankohtaisiin tieteellisiin artikkeleihin ja CSA:n julkaisuihin.

Kolmanteen tutkimuskysymykseen vastattiin systemaattisella kirjallisuuskatsauksella, jossa käytettiin PRISMA-metodia (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Katsaukseen valittiin 18 tutkimusta. Aineisto analysoitiin ja jaettiin viiteen kategoriaan: salaus- ja kryptografiatekniikat (encryption and cryptographic techniques), pääsynhallinta ja tunnistautuminen (access control and authentication), datan eheys ja yksityisyys (data integrity and privacy), pilvien välinen tietoturva (inter-cloud security), sekä monipilviympäristöjen suojaus (multi-cloud security).

Opinnäytetyö tarjoaa ajankohtaisen kirjallisuuskatsauksen pilvidatan tietoturvan nykytilasta.Tulokset osoittavat, että tehokas pilvidatan tietoturva edellyttää teknisten asetusten, sääntelyvaatimusten (regulatory compliance) ja jaetun vastuun onnistunutta yhdistämistä. Kirjallisuudessa kuvatut innovatiiviset teknologiat, kuten hybridisalaus (hybrid encryption), biometrinen tunnistautuminen (biometric authentication), uhkien tunnistusjärjestelmät (threat detection systems) ja varmennettu tiedon poistaminen (verifiable data deletion), vastasivat osaltaan tunnistettuihin haasteisiin. Näiden ratkaisujen yleistettävyyttä rajoittavat kuitenkin metodologiset haasteet. Opinnäytetyössä tunnistetaan myös useita jatkotutkimuksen tarpeita. Näihin kuuluvat jaetun vastuun haasteet resurssien suhteen rajoittuneissa organisaatioissa, kestävyyden huomioiminen pilvi-infrastruktuurien suunnittelussa, sekä uusien teknologioiden vaikutukset pilvipalveluiden tietoturvaan.

Avainsanat: cloud data security, secure data lifecycle, encryption, access control
Sivut 75 sivua ja liitteitä 1 sivu

HAMK
Häme University
of Applied Sciences

Abstract

DP Degree Programme in Business Information Technology
Author Saga Payling-Nyhuus
Year 2025
Subject Recent challenges and solutions in cloud data security
Supervisors Ismo Turve ja Lasse Seppänen

The purpose of this thesis was to examine the current state of cloud data security by identifying its main concepts, key challenges, and recent technological developments. It focused on how cloud data can be effectively managed from the perspective of the cloud service customer, with particular emphasis on data-level protection. The thesis addressed three research questions: (1) What are the main concepts of cloud data security and its management?; (2) What are the main challenges in cloud data security, according to recent research?; and (3) What new technologies to improve cloud data security were introduced between January 2024 and February 2025, and what challenges do they address?. The thesis was not commissioned but was motivated by the limited number of recent literature reviews on this topic and the author's academic interest in cloud computing.

The thesis is theoretical, based on existing research. Chapters 2 to 6 form the theoretical framework of the thesis. Chapters 2 to 5 sought to answer the first research question. The chapters introduce the basics of cloud computing, including service and deployment models, as well as the shared responsibility model. They also present key principles of cloud data security, such as data classification, data states, the secure data lifecycle, and the CIA triad (Confidentiality, Integrity, Availability). Legal and regulatory issues are also discussed. Data security tools from the Cloud Security Alliance (CSA) and Microsoft are examined. Chapter 6 addresses recent cloud data security challenges, focusing on the principles of cloud data confidentiality, integrity, and availability. It highlights risks including unauthorised access, insufficient monitoring, and data exposure in shared environments, citing academic sources and CSA reports. To address the third research question, a systematic literature review was conducted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method. The review focused on empirical research studies published between January 2024 and February 2025. Eighteen studies met the inclusion criteria. The findings were analysed and categorised into five thematic areas: encryption and cryptographic techniques, access control and authentication, data integrity and privacy, inter-cloud security, and multi-cloud security.

Overall, the thesis provides an overview of current cloud data security challenges and solutions. The findings indicate that cloud data security is a constantly evolving field, with added complexity in hybrid and multi-cloud environments. Effective data protection requires a multi-layered approach that integrates technical measures, legal and regulatory compliance, and clearly defined responsibilities between cloud service providers and customers. The systematic literature review identified technologies such as hybrid encryption, biometric authentication, secure data deletion, and intelligent threat detection. While the reviewed solutions were empirically tested, many face limitations in generalisability due to research constraints. The thesis also identifies areas for future research, including challenges of the shared responsibility in resource-limited organisations, sustainability in the design of cloud infrastructures, and the impact of emerging technologies on cloud data security.

Keywords: cloud data security, secure data lifecycle, encryption, access control
Pages 75 pages and appendices 1 page

Contents

Vocabulary

Access control policies
Rules that define who can access specific cloud resources and what actions they can perform on them, based on roles and permissions.

Anonymisation
The process of removing personally identifiable information from data sets, making it impossible to trace the data back to any individual.

Artificial intelligence (AI)
The use of algorithms and machine learning models to simulate human intelligence.

Cloud data breach
A security incident where unauthorised access is gained to sensitive data stored in a cloud environment, resulting in its exposure or theft.

Cloud data security
The practice of protecting data stored in cloud environments from unauthorised access, data breaches, and data loss through various security measures, including encryption, access control, and monitoring.

Cloud Security Alliance (CSA)
A non-profit organisation that develops frameworks, guidance, and certifications to enhance cloud security. It promotes best practices while fostering collaboration between cloud service providers and customers through research, educational programs, and events to address security risks in cloud environments.

Cloud security posture management (CSPM)
Tools and practices to monitor and enforce security policies in cloud environments, ensuring compliance with security standards and best practices.

Cloud service customers (CSC)
Organisations or individuals that use cloud services provided by cloud service providers to store, manage, and process their data.

Cloud service providers (CSP)
Entities that offer cloud computing services, such as infrastructure, platform, or software to customers over the internet.

Cloud storage types
Different types of cloud storage solutions, including object storage, block storage, and file storage, are tailored to different data needs and use cases.

CIA Triad (Confidentiality, integrity, and availability)
A foundational model for managing data security, ensuring that information is kept confidential, accurate, and accessible when needed.

Data classification
The process of categorising data based on its sensitivity and the level of protection required to ensure appropriate security measures are applied.

Data encryption
The process of converting data into a format that is unreadable to unauthorised users, typically using cryptographic algorithms.

Data loss prevention (DLP)
A set of tools and policies designed to prevent sensitive data from being exposed, lost, or shared without authorisation.

Data masking
A technique used to protect sensitive data by replacing it with fictitious or partially obscured values while maintaining the original data's format.

Data remanence
The residual data left behind on storage devices after data has been deleted or overwritten can still be recovered.

Data retention and deletion policies
rules for retaining data for the appropriate duration and securely deleting data when it is no longer needed or when it violates legal or regulatory requirements.

Data sensitivity levels
Categories of data that are assigned based on the potential harm that unauthorised access or exposure could cause, such as highly confidential, confidential, private, and public.

Data security posture management (DSPM)
A set of practices and tools designed to monitor and manage the security posture of data in cloud environments, addressing risks and ensuring data protection.

Data theft
The act of stealing personal, financial, or proprietary data from an organisation or individual, typically with malicious intent for financial gain or espionage.

Disaster recovery plans
A set of procedures and protocols to recover data and resume normal operations in the event of a disaster, ensuring minimal disruption.

Digital signature verification
The process of validating a digital signature to confirm the authenticity and integrity of digital documents or communications.

Encryption protocols
Standards and rules that govern how data should be encrypted and decrypted.

ESG (Environmental, Social, and Governance) standards

ESG standards in the EU are regulatory guidelines that assess a company's environmental impact, social responsibility, and governance practices to promote sustainable and transparent business conduct.

Hybrid cloud
A cloud computing environment that combines on-premises infrastructure with public and/or private cloud services to allow data and applications to be shared between them.

Identity and access management (IAM)
A framework that ensures the right individuals or systems can access the right resources at the correct times, with proper permissions and authentication.

Infrastructure as a service (IaaS)
A cloud computing service model in which a cloud provider offers virtualised computing resources, including servers, storage, networking, and operating systems, over the internet. This enables users to build, manage, and scale their applications without the need for investing in physical hardware.

Incident response plan
A documented strategy for detecting, responding to, and recovering from cybersecurity incidents, ensuring minimal damage and compliance with regulations.

Internet of Things (IoT)
A network of physical devices connected to the internet, which can introduce new security risks as more devices collect, store, and transmit data.

Key management
The process of creating, storing, and managing cryptographic keys used for encryption and decryption to ensure data protection.

Microsoft Azure
A cloud computing service provided by Microsoft offering solutions for computing, networking, databases, and storage.

Multi-cloud
The use of services from multiple cloud providers.

Multi-factor authentication
A security mechanism that requires users to provide two or more verification factors to gain access to a system, enhancing security.

On-demand self-service
The ability for customers to provision and manage cloud resources (e.g., computing power, storage) independently, without requiring human intervention from the service provider.

Platform as a service (PaaS)
A cloud service model that provides customers with a platform to develop, run, and manage applications without having to manage the underlying infrastructure.

Private cloud
A cloud environment dedicated to a single organisation.

Regulatory compliance
Adhering to laws, regulations, and standards that govern data protection, security, and privacy, such as the GDPR and NIS2.

Role-based access control (RBAC)
A method of restricting system access based on the roles of individual users within an organisation, ensuring that users only have access to resources necessary for their role.

Security incident management
The process of identifying, managing, and mitigating security incidents to minimise damage and restore normal operations.

Security monitoring
The continuous observation of systems and networks to detect and respond to potential security incidents or threats.

Shared responsibility model (SRM)
A cloud computing security framework that defines the division of security responsibilities between cloud service providers and customers, depending on the service model.

Security Information and Event Management (SIEM)
Security Information and Event Management (SIEM) tools are software solutions that help organisations detect, analyse, and respond to cybersecurity threats in real time by collecting and aggregating log data from across the IT infrastructure.

Software as a service (SaaS)
A cloud service model in which applications are hosted by the cloud service provider and made available to customers over the internet.

Vendor lock-in
A situation in which an organisation becomes dependent on a specific cloud service provider, making it difficult to switch providers without significant costs or disruptions.

Zero trust (ZT)
Zero trust security is a model that assumes no implicit trust for any user or system, requiring strict identity verification and continuous monitoring for access to resources.

Figures

Tables

Appendices

Liite 1. Aineistonhallintasuunnitelma

1 Introduction

Cloud data security risks have increased due to digitalisation and the rise of cyber threats (Microsoft, 2024, p. 10). Despite the essential role of cloud services in modern-day society, concerns about their data security persist (Alghofaili et al., 2021, p. 32). A HashiCorp survey showed widespread concern among information technology practitioners about cloud data protection and theft (HashiCorp, 2021). According to the Cloud Security Alliance (CSA) (2022b), 57% of the 1,663 surveyed organisations lack confidence in securing cloud-stored data, particularly sensitive information, and nearly half experienced a breach in the past year, with 62% expecting one in the next year (CSA, 2022b, pp.13, 18).

The growing importance of cloud data security is evident in both recent research and the increasing number of regulations. A Google Scholar search for "cloud data security" returned over 2.3 million results, with 53,800 articles published in 2024 alone (Google Scholar, 2025). The European Union Agency for Cybersecurity (ENISA) (2025b) notes that recent years have seen a rapid expansion of EU cybersecurity policies and legislation (ENISA, 2025b).

The shared responsibility model, which assigns the responsibility of securing cloud infrastructure to service providers and data to customers, complicates the data security landscape. This division of responsibilities highlights the importance of understanding how cloud data security is structured and what actions organisations must take to protect their data effectively. (CSA, 2024c, pp. 21-24)

The selection of this thesis topic was influenced by the observation that, despite documentation from cloud service providers such as Microsoft Azure emphasising high levels of cloud security, there are comprehensive cybersecurity reports, including Microsoft (2024) and the ENISA (2024b), that highlight the increasing frequency of cloud-based data security breaches (ENISA, 2024b, p. 6; Microsoft, 2024, p. 10).

The primary aim of this thesis is to explore cloud data security solutions and challenges, with a focus on data-level security from a customer's perspective. It seeks to develop a clearer understanding of cloud data security and to identify areas that may benefit from further research. The thesis was not commissioned but was motivated by the limited

number of recent literature reviews focused specifically on data-level cloud security and the author's academic interest in the topic. This thesis presents a literature review of recent research on data-level cloud security. It is theoretical and reviews existing research. Literature reviews are useful for identifying research gaps, informing hypotheses, and guiding future research (Page et al., 2021, p. 1).

The thesis addresses three research questions:
• What are the main concepts of cloud data security and its management?
• What are the main challenges in cloud data security, according to recent research?
• What new technologies to improve cloud data security were introduced between January 2024 and February 2025, and what challenges do they address?

Chapters 2 to 5 address the first question by reviewing cloud services, data protection methods, and the secure data lifecycle. Chapter 6 addresses the second question by identifying key challenges in cloud data security. The third question is examined in Chapters 7-8 through a systematic literature review using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method, which analyses studies published between January 2024 and February 2025.

2 Cloud computing

The National Institute of Standards and Technology (NIST) (2011) defines cloud computing based on five widely recognised key concepts: resource pooling, broad network access, rapid elasticity, measured service, and on-demand self-service. These key concepts distinguish cloud computing from conventional IT models by enabling the sharing of resources, providing access to services from anywhere, automatically scaling services, offering usage-based billing, and facilitating self-service provisioning. (NIST, 2011, p. 2)

These key concepts are evident in the offerings of major cloud service providers such as Amazon Web Services (AWS) and Microsoft Azure. Both of them offer scalable solutions, which means that the services can automatically adjust to changing workloads. This feature enables businesses to meet demand fluctuations without requiring manual intervention. Automation is another essential feature of these platforms, where processes such as resource provisioning and load balancing are automated. Furthermore, both platforms are based on multi-tenancy. This means that multiple customers share the same physical infrastructure for storing their data. (AWS, 2025; Microsoft, 2025b)

This chapter offers an overview of cloud computing, presenting its key concepts, service models, and deployment models. Furthermore, this chapter introduces the abbreviations CSP and CSC, which will be used consistently throughout the thesis to refer to the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC).

The chapter also discusses the Shared Responsibility Model (SRM), which describes the security roles of CSPs and CSCs in relation to different service models, from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) (CSA, 2024c, pp. 21-23). The information presented in this chapter serves as a basis for addressing the research question: "What are the main concepts of cloud data security and its management?".

2.1 Cloud deployment models

This section examines the primary cloud deployment models and their main features. Cloud deployment models refer to the different ways cloud environments can be deployed depending on an organisation's needs. The most common deployment models are public,

private, hybrid, and multi-cloud. Public clouds are available to the general public and are operated by third-party providers. Private clouds are dedicated to a single organisation, providing greater control over data and security. Hybrid clouds combine both public and private clouds, allowing for greater flexibility in resource management. Multi-cloud environments involve the use of services from multiple cloud providers. (CSA, 2024c, p. 15)

The use of multi-cloud strategies is reported to have increased as organisations seek to optimise their IT operations by deploying services from multiple CSPs. The HashiCorp State of Cloud Strategy Survey (2021) indicates that a considerable number of organisations are adopting multi-cloud environments to enhance flexibility, performance, and reliability. (HashiCorp, 2021)

Each deployment model has distinct advantages and challenges, as described by the Cybersecurity and Infrastructure Security Agency (CISA) (2022). For example, a public cloud offers many cost-saving features, but at the same time, it results in the organisation having less control over data security. A private cloud, in contrast, offers greater control but may require higher capital investment. A hybrid cloud provides a combination of the two. A multi-cloud environment allows organisations to avoid dependency on a single provider, simultaneously mitigating the risks associated with vendor lock-in by distributing workloads across several CSPs. This approach reduces dependency on a single provider and thus might lessen the negative impact of disruptions from service outages or security breaches. (CISA, 2022, pp. 6-8)

Furthermore, CISA (2022) emphasises the importance of a unified security approach in multi-cloud environments. This type of approach, according to CISA (2022), includes centralising security policies, using tools that monitor security across platforms, and standardising log data to ensure consistency. This can increase the complexity of designing multi-cloud systems. (CISA, 2022, pp. 7-8)

2.2 Division of cloud security responsibilities

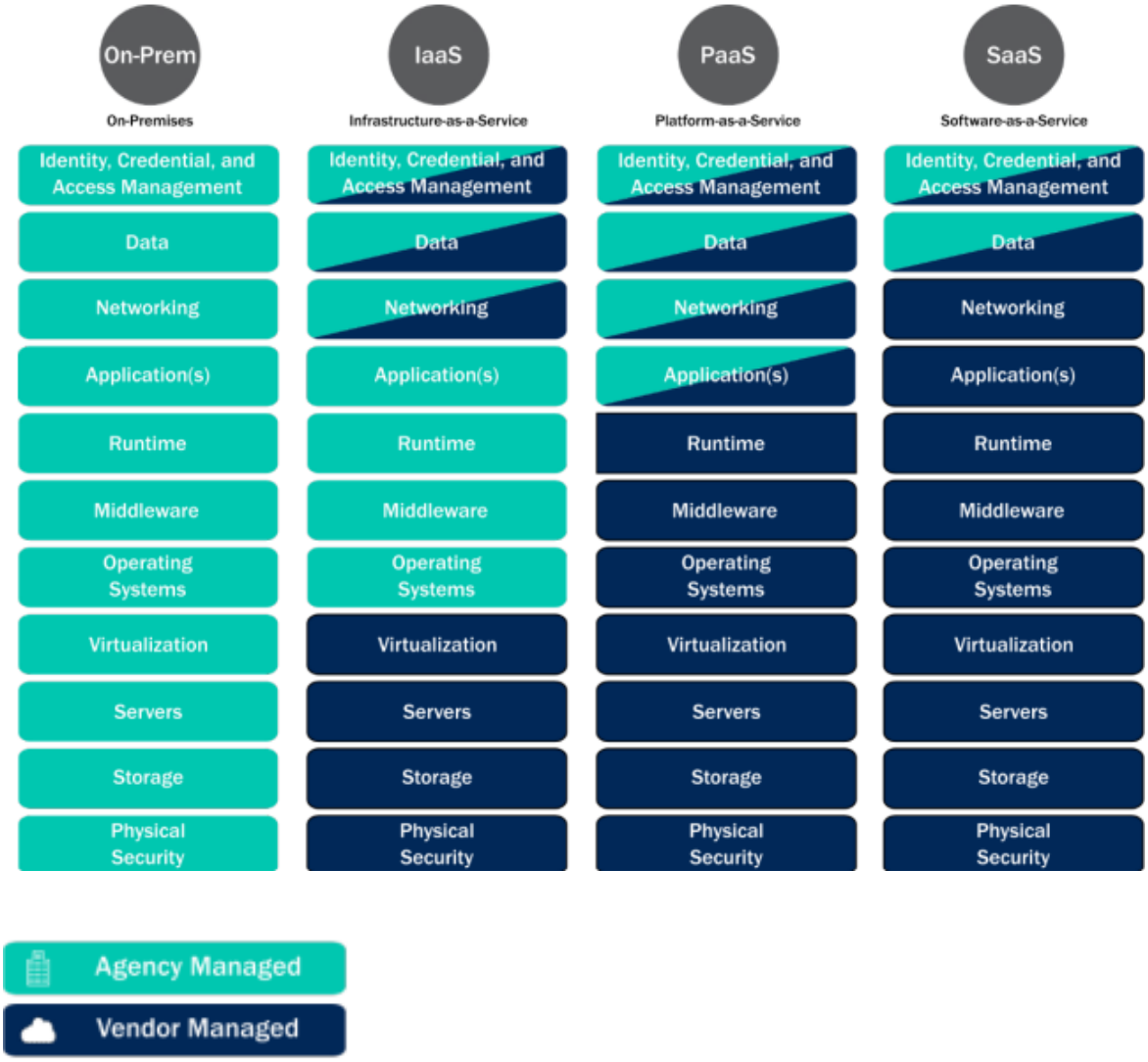
This section explores how security responsibilities are divided between CSPs and CSCs across various cloud service models, utilising the shared responsibility model (SRM) as a framework. Cloud computing services are commonly divided into three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a

Service (IaaS). These models represent different levels of control and responsibility shared between CSPs and CSCs. (CSA, 2024c, p. 14)

The SRM outlines the division of security duties between CSPs and CSCs (CSA, 2024c, p. 21). The security responsibilities between the CSC and CSP shift as organisations transition from SaaS to IaaS, highlighting the importance of understanding these roles to ensure secure cloud environments (CSA, 2024c, pp. 21-23). Similarly, the European Union Agency for Cybersecurity (ENISA) emphasises the importance of defining these responsibilities, particularly to prevent data security incidents (ENISA, 2009b, pp. 8-10).

The CISA (2022) diagram in Table 1 illustrates this shift, showing how the responsibility of the CSP decreases, while that of the CSC increases as organisations move from SaaS to IaaS (CISA, 2022, p. 5). It highlights the increasing responsibility of the customer as they adopt more flexible and customisable cloud service models.

Table 1. Shared Responsibility Model (SRM), which shows how the CSP's (vendor) responsibility decreases and the CSC's (agency) responsibility increases as organisations move from SaaS to IaaS (CISA, 2022, p. 5).



The level of responsibility varies depending on the service model. In SaaS, the CSP handles security aspects, including managing physical infrastructure, maintaining identity management systems, and ensuring platform security through firewalls and antivirus protection. As the service model shifts to IaaS, the CSP's responsibility decreases, and more responsibilities are transferred to the CSC. The CSC becomes responsible for managing guest operating systems, configuring security platforms, and monitoring systems. (ENISA, 2009b, pp. 8-10)

According to the CSA (2024c), CSPs are responsible for securing the underlying cloud infrastructure, which includes data centres, networks, and hardware. In contrast, CSCs are responsible for securing their applications, data, and access controls within the cloud

environment. As organisations transition from SaaS to IaaS, they must implement security controls, manage access, and protect sensitive data. (CSA, 2024c, pp. 21-23)

2.3 Security responsibilities in cloud service models

This section outlines the division of security responsibilities across the cloud service models: SaaS, PaaS, and IaaS. In the SaaS model, security responsibilities are shared between the CSP and the CSC. The CSP is responsible for securing the underlying infrastructure, including the network, servers, and compliance requirements. At the same time, the CSC manages user access and protects sensitive data through controls such as authentication and encryption. (Microsoft, 2024, September 26)

In PaaS, responsibility is also shared between the CSP and CSC. The CSP secures the platform, including infrastructure, middleware, and built-in services. However, unlike in the SaaS model, the CSC retains responsibility for application security, managing user access, and securing sensitive data through controls such as authentication and encryption. (Microsoft, 2024, September 26)

For IaaS, the CSP is primarily accountable for securing the cloud infrastructure, including physical hardware, data centres, and networking components. The CSC, however, is responsible for securing the operating systems, applications, and data within the virtual environment. The CSC has the flexibility to configure and manage virtual machines, networks, and storage resources according to its requirements, but must ensure these resources are appropriately protected. This includes managing access controls, applying security patches to operating systems, and ensuring encryption and protection against unauthorised access. (Microsoft, 2024, September 26)

The division of cloud security responsibilities demands varying levels of security obligations from the CSC depending on the service model. ENISA (2009b) emphasises how organisations must understand these roles in order to effectively secure their data and ensure compliance with relevant regulations. (ENISA, 2009b, pp. 8-10)

2.4 Chapter summary

This chapter explored cloud computing, including its key concepts, service models, and deployment models. It highlighted how cloud computing provides scalability, automation, and resource sharing. (NIST, 2011, p. 2; CSA, 2024c, pp. 14-15)

Additionally, the SRM was introduced, illustrating the division of security responsibilities between CSPs and CSCs. As the division varies across different service models, both parties must understand their roles in maintaining the security of cloud-based systems and ensuring that all security requirements are appropriately addressed. (ENISA, 2009b, pp. 8-10; CSA, 2024c, pp. 21-23; CISA, 2022, p. 5)

The reviewed literature does not explore the possible challenges organisations might encounter when fulfilling security responsibilities across various service models. While this issue is significant, it falls outside the scope of this thesis.

3 Cloud data security

Cloud data security involves different technologies, practices, and regulations aimed at protecting sensitive information across various cloud environments. It protects against threats such as data loss, leakage, breaches, theft, and unauthorised access. Sensitive data includes all information not meant for public sharing, such as personal details, intellectual property, medical records, and biometric data. Cloud data security also covers strategies such as data classification, storage, encryption, and specific security measures adapted to data in different states. (CSA, 2024c, p. 209; Microsoft, 2025a)

This chapter introduces the core principles of cloud data security, focusing on cloud data classification, data states, types of cloud storage, and the concept of the data lifecycle. It also addresses the concept of dark data (CSA, 2022b, p. 8).

The chapter aims to answer the research question: “What are the main concepts of cloud data security and its management?”. The subsequent chapters will explore strategies for securing various types of cloud data at different stages of the data lifecycle.

3.1 Data classification

This section outlines the principles of data classification as a foundational step in managing cloud data security and addresses the concept of dark data. CSA (2024c) explains that data management begins by classifying data based on its sensitivity and importance, which enables organisations to apply the proper security measures to protect each type of data. CSA further states that without clear data classification policies, sensitive information may not be adequately protected, while non-sensitive data may be given unnecessary protection. (CSA, 2024c, pp. 209-210)

Furthermore, dark data refers to untracked, unstructured, and often forgotten information that resides within an organisation’s digital environment. This type of data can take many forms, including outdated employee records, archived transaction logs, unused system files, and email attachments. (CSA, 2022b, p. 8)

Findings from the CSA (2022b) survey of 1663 IT professionals across different organisations globally highlight the widespread nature of the problem of dark data. According to the survey results, a significant number of organisations do not track, monitor, or address unclassified data. However, a large proportion of the study respondents expressed moderate to high concern about dark data and its risks. The survey results indicate that several challenges exist in addressing dark data, including a lack of expertise, insufficient cooperation across departments, and resource constraints. The issue of dark data remains a recognised priority, as 82 per cent of the surveyed organisations considered managing dark data to be of moderate to high importance. CSA (2022b) concludes that the survey results indicate a growing need for clear data classification policies, thereby reducing data security risks. (CSA, 2022b, p.15)

The CSA explains that data is usually classified into four categories: highly confidential, confidential, private, and public. These categories represent different levels of sensitivity: very high, high, moderate, and low, based on the potential harm that could result from unauthorised access. Table 2 illustrates these categories. (CSA, 2024c, pp. 209-210)

Table 2. Data classification scale illustrating categories from low to very high based on sensitivity, adapted from CSA Security Guidance for Cloud Computing (CSA, 2025, p. 210).

More controls and monitoring		
Highly confidential	Most sensitive data that could cause severe damage	**Very high sensitivity**
Confidential	Data that could cause significant harm if exposed	**High sensitivity**
Private	Data intended for internal use, could cause harm	**Moderate sensitivity**
Public	Data that can be disclosed to public without risk	**Low sensitivity**
Less controls and monitoring		

The consequences of public and private data exposure are typically less severe than those of confidential and highly confidential data (CSA, 2025, p. 210). Newhouse et al. (2023) further elaborate that data classification is crucial for structuring data security management based on an accurate assessment of sensitivity levels (Newhouse et al., 2023, p. 7).

Classification structures allow organisations to protect data by implementing targeted protection strategies based on the assessed risk levels. This is also important for regulatory compliance, as sensitive data requires specific protection methods. Additionally, CSA states that data classification needs to be a dynamic and ongoing process as the legal and operational environments evolve. (CSA, 2024c, pp. 209-210)

3.2 Data states and cloud infrastructure levels

This section examines the fundamental aspects of data states and the layered security measures within cloud infrastructure. This thesis specifically concentrates on the data layer of cloud infrastructure, emphasising that, although other infrastructure levels should be considered for effective cloud data security, they are excluded from this analysis due to scope limitations.

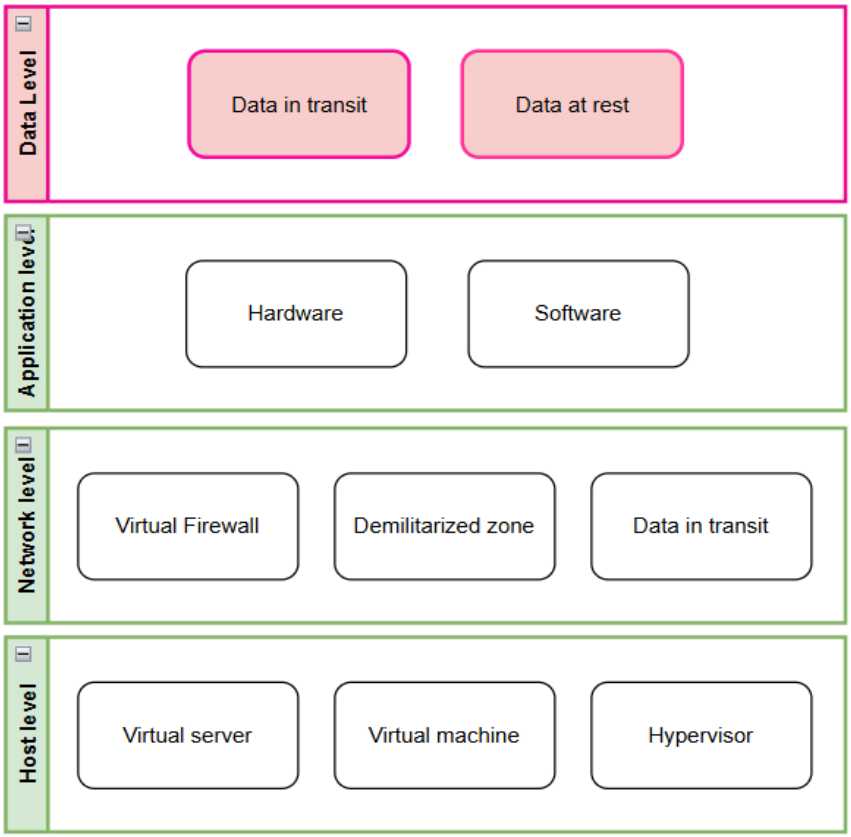
The CSA (2024c) explains that data classification and its states form a foundational framework for implementing security measures based on the context (CSA, 2024c, pp. 210-211). Algofaili (2021) explains that securing data in all its states is essential to prevent issues such as data breaches, theft, or corruption (Algofaili, 2021, p. 13).

According to the CSA (2024c), data exists in three primary states: at rest, in motion, and in use. Data at rest refers to data that is stored in databases, file systems, or cloud environments. Security measures for this type of data include encryption, access controls, and regular backups. Data in motion, also known as data in transit, refers to data being transmitted across networks, such as when sending emails or accessing online files. This type of data is vulnerable to network-based attacks, including sniffing or man-in-the-middle attacks. It requires encryption protocols and secure communication channels to ensure that it remains private and unaltered during transfer. Data in use involves information that is actively accessed, processed, or viewed. It is protected through mechanisms such as access control, user activity monitoring, and endpoint protection. Addressing security across these three data states — at rest, in motion, and in use — supports comprehensive data protection. Each state requires distinct security approaches due to the different conditions in which the data exists. (CSA, 2024c, pp. 210-211)

Concerning the levels of cloud infrastructure, Saini & Saini (2014) explain that cloud infrastructure security operates on multiple levels, including data, network, and computing. They state that data security in cloud computing involves protecting information when it is stored (data-at-rest), transmitted across networks (data-in-transit), and deleted, to prevent unauthorised access or data loss. (Saini & Saini, 2014, pp. 3-4)

The Saini & Saini (2014) perspective differs from the more recent CSA (2024c) definition introduced earlier in the paragraph regarding the three data states, indicating that the understanding of cloud data is evolving and varies slightly in the literature. The layered nature of cloud infrastructure security is further demonstrated in Figure 1, which depicts various security procedures implemented across the different layers: data, application, network, and host levels (Algofaili et al., 2021, p. 11). Here, two data states are considered.

Figure 1. Cloud Infrastructure levels illustrating the security mechanisms employed at the data, application, network, and host levels, adapted from Algofaili et al. (2021) (Algofaili et al., 2021, p. 11).



3.3 Types of cloud data storage

This section briefly describes common cloud data storage types. Data classification and data states are closely connected to various cloud storage solutions, each designed to meet different data needs. The types of cloud storage include, for example, object storage, volume storage and database storage. By leveraging these cloud storage solutions and implementing recommended security measures for data in its different states, organisations can enhance the protection of their sensitive data. (CSA, 2024c, p. 211)

For instance, an example of object storage is Microsoft Azure Blob Storage, which is optimised for storing unstructured data, such as images, videos, and backups. Volume storage is represented by Azure Managed Disks, which serve as virtual hard drives for Azure Virtual Machines, supporting operating system files and application data. Database storage is offered through services such as Azure SQL Database, a managed relational database platform supporting structured and semi-structured data. These services align with various data classification and protection requirements in the cloud environment.

(CSA, 2024c, p.212; Microsoft, 2023, October 11; Microsoft, 2025, April 2; Microsoft, 2025, April 4)

3.4 The concept of data lifecycle

This section explores the concept of the data lifecycle, offering an overview of its stages. Understanding the data lifecycle helps in choosing suitable privacy and security strategies. Each stage of the data lifecycle presents particular risks to data security, and understanding these stages enables organisations to implement cloud data protection more effectively. Although no universally accepted standard defines the data lifecycle, several models have been suggested. The CSA (2024) reviewed different models proposed by NIST (2023) and produced a summary that brings together the key stages shared across these models, shown in table 3. (CSA, 2024a, p. 6)

Table 3. Summary of NIST-proposed data lifecycle models combining the key stages found in each, adapted from CSA (CSA, 2024a, p. 6).

4 Stage	5 Stage	7 Stage	8 Stage
Creation	Creation	Plan	Generation
Usage	Storage	Creation	Collection
Storage	Usage	Manage	Processing
Archive and deletion	Archiving	Use	Storage
	Destruction	Share	Management
		Collect	Analysis
		Destroy	Visualisation
			Destruction

The different data lifecycle models listed in Table 3 vary from simple four-stage frameworks to more detailed models with up to eight stages. Simpler models highlight the most essential phases, while more complex ones address specific tasks and processes in more detail. Selection of the model depends on the organisation's needs, with large organisations generally requiring more complex models. (CSA, 2024a, p. 5)

As an example of a data lifecycle at its simplest form, NIST proposes a four-phase model comprising the following phases: identify, use, maintain, and dispose. In the identification phase, organisations locate and classify their data assets. Labelling and classifying data carefully ensures that the proper access controls and security measures are used. The use phase includes accessing, modifying, sharing, or reusing data. During this phase, new data may also be generated by aggregating or transforming existing information. The maintenance phase focuses on preserving the usability of data over time. The final disposal phase includes the destruction of data when it is no longer required. (Newhouse et al., 2023, pp. 2-3)

Understanding and actively managing the data lifecycle enhances the protection of sensitive data and compliance with legal and regulatory requirements. Additionally, the risk of data loss or misuse decreases. (CSA, 2024a, p. 22)

3.5 Chapter summary

This chapter introduced key principles of cloud data security, covering aspects such as data classification, data states, and cloud storage types. It highlighted the importance of effective data classification and management in enhancing data security and mitigating data security-related risks. The chapter also explored the concept of dark data, emphasising the importance of effective data classification, which allows for appropriate security measures based on the data's sensitivity. (CSA, 2022b, p.8, 15; CSA, 2024c, pp. 209-212)

Furthermore, the chapter examined the data lifecycle, stressing the importance of managing data from creation to disposal to ensure both security and compliance. It discussed how each stage of the data lifecycle requires specific considerations to protect the data and maintain its integrity, particularly in cloud environments. By understanding and implementing effective data management strategies, organisations can better protect their data and comply with regulatory requirements. (CSA, 2024a, p. 6, 22; Newhouse et al., 2023, pp. 2-3)

While the reviewed literature offers a good foundation for understanding cloud data security principles, it does not address the practical challenges organisations may face in applying

these principles across various service models. Researching these significant challenges is beyond the scope of this thesis.

4 Cloud data security management

Securing cloud data throughout its lifecycle involves several stages, with the principles of confidentiality, integrity, and availability — commonly known as the CIA triad — providing a framework for managing cloud data security (CSA, 2024a, pp. 12-14). These principles are central not only to effective cloud data management but also to various European Union (EU) regulations, such as the General Data Protection Regulation (GDPR) (Regulation 2016/679 of the European Parliament and of the Council), the NIS2 Directive (Directive 2022/2555 of the European Parliament and of the Council), and the Cyber Resilience Act (Regulation 2024/2847 of the European Parliament and of the Council) (European Commission, 2022; European Parliament & Council of the European Union, 2016, 2024). To uphold the CIA triad, organisations rely on established governance models and security practices, supported by recognised security frameworks such as NIST Cybersecurity Framework (CSF) and ISO/IEC 27001:2022 (ENISA, 2024a, p. 22).

This chapter introduces the CSA Compliance Checklist for Data Lifecycle Management, outlining key requirements for securing data in line with CSA guidance (CSA, 2024a, pp. 17–18). Additionally, it examines how governance frameworks, legal regulations, and best practices align with EU regulations, particularly the GDPR. Given the growing importance of environmental responsibility, the chapter includes a section on sustainability in cloud infrastructure, examining ways to reduce the environmental impact of cloud services. The chapter seeks to answer the research question: ”What are the main concepts of cloud data security and its management?”.

4.1 Cloud data lifecycle management requirements

This section outlines the core requirements for effective cloud data lifecycle management, as identified by the CSA (2024a). According to them, effective cloud data management requires well-established governance and security measures to ensure the confidentiality, integrity, and availability of data throughout its lifecycle. Data governance, which includes the creation of policies and procedures for accessing, storing, processing, and sharing data, is vital for maintaining security and ensuring legal compliance. (CSA, 2024a, p. 14)

Table 4 provides a summary of the key components of the compliance checklist proposed by CSA for effective data lifecycle management. (CSA, 2024a, pp. 17–18).

Table 4. Compliance Checklist for Data Lifecycle Management, adapted from CSA (2024a, pp. 17-18).

Category	Description
Data Classification	Identify and tag sensitive data types using automated tools for classification and metadata tagging.
Access Control Policies	Implement access control, enforce least privilege principles, conduct periodic access reviews, and revoke unused privileges.
Regular Audits	Perform internal and external compliance audits, audit third-party vendors, and utilise Security Information and Event Management (SIEM) tools for compliance reporting and anomaly detection.
Incident Response Plan	Develop a detailed incident response plan (IRP), train staff, and regularly test the IRP through simulated scenarios.
Training and Awareness	Conduct cybersecurity training, phishing simulations, provide role-specific compliance updates, and foster awareness of regulatory requirements.
Data Retention and Deletion	Define retention schedules that align with regulations, utilise certified destruction methods, and enforce deletion policies for obsolete data.
Encryption Standards	Encrypt data at rest, in transit, and during processing using modern encryption protocols, and consider quantum-resistant encryption.
Backup and Recovery	Maintain periodic backups with secure encryption, regularly test disaster recovery plans, and ensure compliance with data sovereignty laws for backups.
Monitoring and Logging	Deploy centralised monitoring systems (e.g., SIEM), enable detailed logging for critical systems, and utilise anomaly detection tools.
Third-Party Compliance	Conduct due diligence for vendor selection, include compliance requirements in contracts, and ensure vendors adhere to compliance standards.

As previously mentioned in the thesis, appropriate data classification systems enable the identification of sensitive data and thus the application of appropriate access controls to prevent unauthorised access, which is also highlighted in Table 4. Encryption plays an equally important role, as it protects data both at rest and in transit. Table 4 also lists regular audits and continuous monitoring, which further support the early identification of security risks and enhance cloud data security. Table 4 shows several essential practices for managing the data lifecycle. These include regular cybersecurity training and conducting phishing simulations. Data retention and deletion policies must align with

applicable legal requirements, such as those outlined in the GDPR. Additionally, backups must be encrypted, disaster recovery plans must be tested, and compliance with sovereignty laws must be ensured for backups. Continuous monitoring, detailed logging, and the deployment of anomaly detection tools are also included. Lastly, Table 4 states that third-party vendors should undergo thorough assessments, with compliance terms incorporated into contracts and regular audits conducted to ensure adherence to security standards. (CSA, 2024a, pp. 16–18)

4.2 European Union cybersecurity legislation

While numerous EU regulations are relevant to the topic of cloud data security, this thesis presents only a selection of them due to scope limitations. The following section offers an overview of key EU cybersecurity laws that complement the GDPR, which serves as the primary legal framework examined in this study. The GDPR was selected for its prominence as a leading data protection regulation in the EU, and it mandates strict data security measures to protect individuals' personal information, particularly in cloud computing environments (Regulation 2016/679 of the European Parliament and of the Council). Findings from the CSA Data Security Risk Survey (2025) support this, indicating that regulatory compliance is vital for effective cloud data risk management (CSA, 2025, p.11). The survey shows that 59% of respondents view regulation and compliance as essential to reducing data security risks, with the GDPR often cited as a key regulatory framework (CSA, 2025, p.11). While the GDPR is the primary focus due to the scope limitations of this thesis, other EU cybersecurity laws also play essential roles in ensuring required data protection practices within cloud environments, some of which will be briefly outlined below (European Commission, n.d.).

The EU Cybersecurity Strategy aims to enhance resilience against cyber threats and ensure the security of digital technologies. This strategy focuses on safeguarding critical services, including healthcare facilities, energy networks, and connected devices, while strengthening the EU's collective ability to respond to cyberattacks. (European Commission, n.d.)

Effective from October 2024, the NIS2 Directive addresses cross-border cybersecurity risks by requiring Member States to oversee and collaborate in protecting cloud services and other critical digital infrastructure (Directive 2022/2555 of the European Parliament and of

the Council). The Cyber Resilience Act, which came into force in December 2024, establishes mandatory cybersecurity standards for digital products, including those used in cloud environments (Regulation 2024/2847 of the European Parliament and of the Council). Manufacturers of connected products are required to implement security measures throughout the product lifecycle to meet EU security standards (Regulation 2024/2847 of the European Parliament and of the Council).

Entering into force on February 2025, the Cyber Solidarity Act (Regulation 2025/38 of the European Parliament and of the Council) enhances the EU's ability to respond to large-scale cybersecurity incidents affecting cloud services. It establishes a European Cybersecurity Alert System and a Cybersecurity Emergency Mechanism, which includes a reserve of trusted incident response services. (Regulation 2025/38 of the European Parliament and of the Council)

According to ENISA (2025b), a significant number of cybersecurity laws within the European Union are relatively recent, with additional regulatory measures currently under development. This highlights a growing need for cloud data protection. ENISA (2025b) states that its objective is to enhance cybersecurity across the European Union, particularly as new cybersecurity regulations are introduced and cyber threats continue to escalate globally. (ENISA, 2025b)

4.3 Cybersecurity frameworks

This section examines the role of established cybersecurity frameworks in protecting cloud data, using the NIST Cybersecurity Framework (CSF) as an example. The European Union Agency for Cybersecurity (ENISA, 2024a) emphasises the importance of security frameworks in protecting data throughout its lifecycle. Among the widely recognised frameworks are the NIST CSF and the ISO/IEC 27001:2022 standard, developed by the International Organisation for Standardisation (ISO), which offers flexible guidance that organisations can adapt to their specific needs. These frameworks support the implementation of EU cybersecurity laws by providing adaptable approaches to managing cybersecurity risks. (ENISA, 2024a, p. 29; ISO/IEC 27001, 2022)

Furthermore, the NIS2 Directive encourages organisations to adopt established frameworks for cybersecurity risk management, although it does not mandate the use of a

specific framework. It emphasises the need to apply such models to ensure compliance with cybersecurity requirements. (ENISA, 2024a, p.16)

More specifically, Article 21 of the NIS2 Directive details specific measures that entities must implement, including risk analysis, information system security, incident management, business continuity, supply chain security, and security during system development. Entities must also evaluate the effectiveness of their cybersecurity measures, adopt basic security practices, provide training, use encryption, enforce access controls, manage assets efficiently, and implement multi-factor authentication and secure communication systems. (Directive 2022/2555 of the European Parliament and of the Council)

The NIST CSF is a flexible and practical model that aligns with key European regulations, including the GDPR and NIS2 (ForeNova, 2024). NIST further explains that the CSF 2.0 is suitable for managing cloud data security within cloud environments, emphasising that cybersecurity is a continuous and dynamic process (NIST, 2024, pp. 2-4).

The NIST CSF comprises six interrelated functions: govern, identify, protect, detect, respond, and recover, which form a continuous cycle to reflect their mutual interdependence. The CSF is designed to be adaptable and is intended for use by organisations of all sizes. However, it should be implemented in conjunction with other resources, such as standards, guidelines, and best practices, to support comprehensive management of cybersecurity risks at the enterprise level. (NIST, 2024, pp. 2-4)

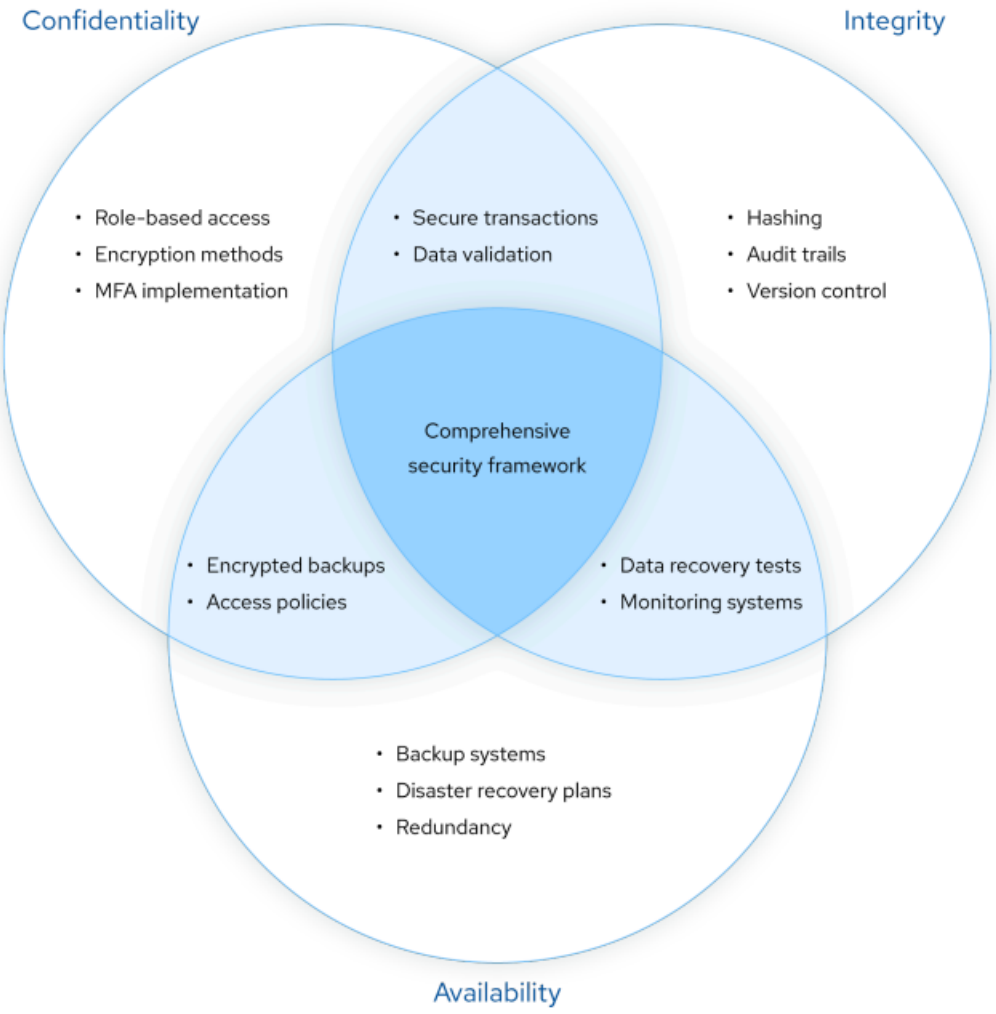
Figure 2. The NIST Cybersecurity Framework 2.0 (NIST CSF) is represented as an interconnected wheel (NIST, 2024, p. 10).

According to NIST (2024), the "govern" function serves as the foundational element, supporting the other functions. The "identify," "protect," and "detect" functions focus on securing systems, and the "respond" and "recover" functions are essential for managing security incidents and recovering from them. The functions are arranged in a circular design, which illustrates the continuous and interdependent nature of these different functions, allowing the system to adapt to improvements in cybersecurity management. (NIST, 2024, pp. 3-4)

4.4 The CIA Triad in cloud data security

The CSA (2024a) asserts that the CIA triad is a foundational framework for protecting data throughout its lifecycle, providing a practical guide for selecting security tools and technologies that help protect data at each stage of the data lifecycle. Figure 3 illustrates how the three principles of the triad—namely, confidentiality, integrity, and availability—work together to secure data. It also outlines some of the key tools and technologies used to protect data in cloud environments, while illustrating how these principles intersect to form a comprehensive framework for cloud data security. (CSA, 2024a, pp. 12-14)

Figure 3. CIA triad as presented by the CSA (CSA, 2024a, p. 12).



The literature emphasises the need to strike a balance between these principles to ensure that data is both secure and accessible when needed (CSA, 2024a, p. 14). Similarly, the GDPR stresses the need to balance key data protection principles for lawful data processing. If confidentiality is overemphasised, it may restrict legitimate data access. On the other hand, limiting data availability could limit individuals' rights to access their data, as outlined in Article 15 of the GDPR (Regulation 2016/679 of the European Parliament and of the Council).

This section introduces the CIA triad as defined by the CSA (2024a). It explores its application within cloud environments and how it aligns with regulatory frameworks such as the GDPR (CSA, 2024a, pp. 12-15). Each principle of the CIA triad will be described, emphasising its role, challenges, and practical measures for implementation in cloud-based systems.

4.4.1 Confidentiality

This subsection examines the principle of confidentiality as a fundamental aspect of cloud data security. Cloud data confidentiality is a key security principle that ensures sensitive data stored, processed, or transmitted in cloud environments is protected from unauthorised access, disclosure, or misuse. The confidentiality principle ensures only authorised individuals or systems can access sensitive data, thus protecting it from being viewed or stolen by unauthorised parties. (CSA, 2024a, p.12)

The confidentiality principle is supported by regulatory frameworks such as the GDPR, which requires organisations to implement strong protection to maintain data confidentiality throughout its lifecycle. GDPR specifies that personal data processing must be lawful, fair, and transparent, based on valid legal grounds such as the individual’s consent, necessary for the performance of a contract, or based on one of the other legal bases for processing data mentioned in Article 6. Furthermore, Article 32 obliges organisations to adopt appropriate technical and organisational measures to secure data. (Regulation 2016/679 of the European Parliament and of the Council)

To maintain confidentiality, the GDPR recommends practices such as data encryption and strict access controls, as detailed in Article 32, which focuses on the security of processing. This article requires data controllers and processors to implement appropriate measures that ensure a level of security commensurate with the risk (Regulation 2016/679 of the European Parliament and of the Council).

A survey by Alghofaili et al. (2021) reveals that issues related to cloud data confidentiality are on the rise, especially because more people are using shared cloud systems. The compromise of one system could potentially lead to compromises in other systems. (Alghofaili et al., 2021, p. 16)

4.4.2 Integrity

This subsection explores the principle of data integrity in cloud environments. Data integrity, as defined by NIST, refers to "the property that data has not been altered or destroyed in an unauthorised manner" (Cawthra et al., 2020, p. 32). In the context of cloud

computing, this principle ensures that data remains accurate, consistent, and trustworthy over time (CSA, 2024a, p. 13).

To preserve data integrity, various security measures must be implemented, including cryptographic techniques, error detection mechanisms, and access controls, to prevent unauthorised modifications or misuse of data. Integrity monitoring enables organisations to detect, analyse, and respond to unauthorised alterations within data in their systems. For such monitoring to be effective, it is essential to establish a baseline of file and system integrity before any incidents occur. (Cawthra et al., 2020, p. 19)

This focus on data integrity aligns closely with the GDPR. It provides that personal data must be kept accurate and up-to-date as outlined in Article 5, and that organisations implement measures to prevent unauthorised changes to data. (Regulation 2016/679 of the European Parliament and of the Council)

Tools such as checksums and audit trails can be used to track who accessed or modified data. Data immutability, on the other hand, where data cannot be changed without detection, can also be employed to protect the trustworthiness of the data. These practices can help organisations comply with GDPR requirements and maintain the accuracy and reliability of their data. (CSA, 2024a, p. 13)

Furthermore, Alghofaili et al. (2021) emphasise the importance of public audits in verifying the integrity of cloud data. They also discuss the challenge of preventing privacy leakage when involving third-party auditors. (Alghofaili et al., 2021, p. 30)

4.4.3 Availability

This subsection discusses the principle of availability in cloud data security. According to the NIST, availability is defined as “ensuring timely and reliable access to and use of information” (NIST, 2011). The principle of cloud data availability relates to the reliable and prompt access to data stored in the cloud by authorised users, even during disruptions or technical failures (CSA, 2024a, p. 13).

The importance of availability is also emphasised by the GDPR, which recognises the right of individuals to access their data under Article 15. Furthermore, Article 32 provides that

organisations must implement measures to guarantee data availability during emergencies or system failures. (Regulation 2016/679 of the European Parliament and of the Council)

Achieving availability in cloud computing requires implementing strategies such as system redundancy, regular data backups, and failover mechanisms to ensure uninterrupted service. These measures are essential for minimising downtime and ensuring continuous access to critical information. (CSA, 2024a, p. 13)

In line with these requirements, Alghofaili et al. (2021) identify three major threats to data availability: network-based attacks, the reliability of cloud service providers, and vulnerabilities in third-party backups. They recommend using data redundancy, such as storing duplicate copies of data across multiple locations or systems, as a strategy to maintain uninterrupted access to data in the event of failures or cyberattacks. (Alghofaili et al., 2021, p. 35)

4.5 Securing the cloud data lifecycle

This section explores secure cloud data management across its lifecycle, emphasising the CIA triad and its alignment with the GDPR. The findings of the CSA Data Security Risk Survey (2025) reinforce the importance of regulatory compliance in managing data security risks, with the GDPR identified as a key framework (CSA, 2025, p. 11).

Following the CSA's seven-stage model of a data lifecycle, each stage—planning, data acquisition, storage, use, sharing, archiving, and destruction—is examined in the context of cloud data management (CSA, 2024a, pp. 6-10). The GDPR is referenced throughout the discussion to illustrate its practical application in supporting cloud data lifecycle management.

4.5.1 Early stages: planning, acquisition, and storage

This section explores the initial phases of the cloud data lifecycle—planning, acquisition, and storage—highlighting the foundational role these stages play in establishing effective data governance. The planning stage involves defining roles, responsibilities, and decision-making authority regarding data access, quality, retention, and security. At this stage,

organisations also classify data and align data practices with business needs and legal frameworks. (CSA, 2024a, p. 6)

Under GDPR, organisations must establish a lawful basis for data processing, conduct Data Protection Impact Assessments, and define data governance roles according to Articles 5 and 30 of the GDPR (Regulation 2016/679 of the European Parliament and of the Council). Data governance tools, such as Role-Based Access Control (RBAC) and data classification systems, can be used to manage data and ensure regulatory compliance (CSA, 2024a, p. 6).

The cloud data lifecycle starts with the data acquisition stage, which is essential for establishing security measures aligned with the CIA triad: confidentiality, integrity, and availability. Techniques such as input validation, encryption, and secure transmission protect data from tampering, unauthorised access, and loss. (CSA, 2024a, p. 7)

Assigning data sensitivity levels (e.g., private or confidential) enables the implementation of appropriate access controls and ensures compliance with regulatory requirements. Key risks at the data acquisition stage include data corruption, injection attacks, and insecure handling of sensitive information. Strategies to mitigate these risks include cryptographic integrity checks and collecting only essential data. Tools such as automated data classification, metadata tagging, and data inventories support these requirements. (CSA, 2024a, p. 7)

Compliance with the GDPR is also important. Article 5 outlines seven key principles for the lawful processing of personal data and mandates data minimisation, while Articles 12-14 specify the information that must be provided to data subjects and require communications to be in a concise, transparent, intelligible, and easily accessible form. (Regulation 2016/679 of the European Parliament and of the Council)

Data storage in the cloud involves both technical safeguards and legal compliance (CSA, 2024c, pp. 222-223). Under the GDPR, Article 32 requires the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Regulation 2016/679 of the European Parliament and of the Council).

During the storage phase, the primary goal is to ensure that data remains secure from unauthorised access while being accessible to the entities that have the right to access it. Standard security measures include encryption, pseudonymisation, and access controls, with redundancy mechanisms such as replication and backups. (CSA, 2024c, pp. 222-223)

4.5.2 Data use and sharing

This section examines the use and sharing stage of the cloud data lifecycle. The use stage of the data lifecycle involves accessing, processing, and analysing data. During this stage, maintaining the confidentiality and integrity of data is a primary concern, particularly in environments where multiple users or systems interact with sensitive information. Security controls aim to ensure that only authorised users can access or modify data, and that any changes are traceable. This phase may also involve constraints related to data localisation or contractual agreements, requiring clear documentation of how and where data can be used. (CSA, 2024a, p. 8)

According to Articles 5 and 6 of the GDPR, organisations must ensure that data processing is lawful, fair, and transparent, based on valid legal grounds. These grounds may include the individual’s consent, the necessity of processing for the performance of a contract, or one of the other legal bases for data processing outlined in Article 6 of the GDPR. (Regulation 2016/679 of the European Parliament and of the Council)

Data sharing involves the exchange of information between internal teams, external partners, and third-party providers; however, it also introduces data security and regulatory compliance risks, particularly when sensitive data leaves the organisation's control (CSA, 2024a, p. 8). Under the GDPR, data controllers must establish Data Processing Agreements (DPAs) with third parties processing personal data on their behalf (Article 28) (Regulation 2016/679 of the European Parliament and of the Council).

To protect shared data, organisations can utilise encryption, RBAC, and strong authentication protocols, along with secure transport methods, to safeguard data in transit. Technologies enabling real-time access without data duplication support data integrity and efficiency. (CSA, 2024a, p.9)

The CSA (2022b) reports that 58% of incidents involved third parties, and 81% of organisations express moderate to high concern over access risks, as many grant third parties similar access to internal users. As cloud adoption and reliance on third parties grow, securely managing data sharing in compliance with regulations becomes increasingly complex. (CSA, 2022b, p.7)

4.5.3 Later stages: archiving, disposal and destruction

This section explores the final stages of the cloud data lifecycle, focusing on the processes of data archiving, disposal, and destruction. Archived data, which is no longer actively used, is stored in separate systems for long-term retention and may follow a distinct data lifecycle to meet requirements for compliance, historical analysis, or future use. Examples of challenges in data archiving include ensuring long-term data accessibility and integrity, protecting data from unauthorised access, and managing the scalability and cost-efficiency of storage solutions. Encryption is essential for meeting compliance requirements and maintaining data confidentiality, while regular audits and access controls support the ongoing security of archived information. (CSA, 2024a, pp. 9-10)

The final stage of the data lifecycle is data disposal and destruction, which aims to ensure that data is permanently deleted or destroyed to prevent unauthorised access and misuse of discarded data. Best practices, such as certified destruction methods and appropriate record-keeping, help secure irreversible data deletion and destruction. Appropriate data deletion also ensures compliance with data privacy laws. (CSA, 2024a, p. 10)

The GDPR mandates that organisations ensure the irreversible erasure of data, as outlined in Article 17. It also requires organisations to implement appropriate document destruction methods. (Regulation 2016/679 of the European Parliament and of the Council)

Aissaoui et al. (2017) discussed the issue of residual data in their survey, questioning how organisations can ensure that data is truly deleted adequately from remote servers when requested. Data remanence, defined as the presence of residual data even after deletion, reformatting, or reallocation to another person, remains a significant concern in cloud environments. (Aissaoui et al., 2017, p. 1)

4.6 Sustainability in cloud infrastructure

This section offers a brief examination of developments in sustainability in cloud infrastructures. It is not meant to be comprehensive but aims to summarise recent trends. As cloud computing continues to grow, its environmental impacts are becoming more significant (Smith & Nakagawa, 2025). The Cloud Security Alliance (CSA) highlights sustainability as a core pillar, alongside security, operational excellence, and cost optimisation (CSA, 2024a, p. 148). The CSA recommends reducing environmental impact by enhancing resource efficiency, minimising waste, and maximising utilisation (CSA, 2024a, p. 148). The United Nations Global Compact also urges organisations to adhere to core principles relating to human rights, labour standards, environmental protection, and anti-corruption (United Nations Global Compact, n.d.). Additionally, frameworks such as the Global Reporting Initiative (GRI) Standards guide reporting on environmental, social, and governance (ESG) issues, thereby promoting transparency and trust with stakeholders (Global Reporting Initiative, 2023). Regulation (EU) 2024/3005 of the European Parliament and of the Council (2024b) introduces stricter requirements for ESG rating agencies, demanding clearer and more reliable reporting (Regulation (EU) 2024/3005 of the European Parliament and of the Council).

These recent developments highlight that environmental impact continues to be a concern. Regarding cloud data, data centres use large amounts of energy and resources. This issue is worsened by underused hardware and inefficient systems, which increase carbon emissions and operational risks further, necessitating careful cloud data governance and innovative technological solutions to address the problem. (Storj, 2023, pp. 4-11)

Organisations are increasingly adopting measures to reduce their environmental footprint. For instance, Microsoft’s 2025 Environmental Sustainability Report highlights progress towards its 2030 targets, including a 29.9% reduction in Scope 1 and 2 emissions and expanded agreements for renewable energy. However, overall emissions have risen due to increased demand for AI and cloud services. (Smith & Nakagawa, 2025)

To summarise, the section highlights growing concerns regarding the environmental footprint of cloud infrastructures, emphasising the need for sustainable cloud data management aligned with ESG standards and evolving digital sustainability regulations. It

also identifies a rising demand for innovative solutions to reduce carbon emissions and minimise resource waste. (CSA, 2024a, p. 148; Storj, 2023, pp. 12-17)

The example illustrates that, despite companies such as Microsoft successfully reducing their direct emissions, overall emissions may still rise due to increasing demand for cloud services. This highlights the need for technological innovation in addition to resource optimisation. (Smith & Nakagawa, 2025)

4.7 Chapter summary

This chapter provided an overview of cloud data security management. It focused on the principles of the CIA triad (CSA, 2024a, pp. 12-15). It introduced the CSA Compliance Checklist for Data Lifecycle Management, which emphasised practices such as data classification, access controls, encryption, audits, and incident response (CSA, 2024a, p.12-14). The chapter also discussed data governance and security measures as crucial for ensuring legal compliance and mitigating data security risks (CSA, 2024a, p.14; ENISA, 2024a, p. 22).

The chapter further examined key EU cybersecurity laws, especially the GDPR, and its impact on cloud data security, stressing the need for secure data processing and sharing (Regulation 2016/679 of the European Parliament and of the Council). It also explored the importance of security frameworks, such as NIST CSF and ISO/IEC 27001:2022, for guiding organisations in protecting data throughout its lifecycle (ENISA, 2024a, p. 29). Lastly, it covered the seven stages of the data lifecycle, from planning and acquisition to disposal, outlining how secure data management practices can ensure compliance with legal standards (CSA, 2024a, pp. 6-10).

Additionally, the chapter acknowledged growing concerns about the environmental impact of cloud infrastructure, highlighting the importance of sustainable cloud data governance and innovative solutions to reduce carbon emissions and resource waste. Compliance with ESG standards and emerging sustainability regulations plays an important role in cloud service management. (CSA, 2024a, p. 148; Storj, 2023, pp. 12-17).

Although the reviewed literature outlines various frameworks and recommended practices, it does not offer a definitive approach to achieving effective cloud data security

management and compliance. This suggests that organisations must interpret and apply these principles according to their specific needs, highlighting the importance of careful planning of cloud data security management.

5 Cloud data security tools and technologies

This chapter addresses the study question, "What are the main concepts of cloud data security and its management?" by providing an overview of the central cloud data security tools and technologies. First, it presents the CSA-recommended essential tools for securing the data lifecycle (CSA, 2024c, pp. 213-214). Then, the chapter delves into Microsoft tools as recommended in Microsoft's Cloud Security Benchmark for data protection (Microsoft, 2025, April 23).

Both the CSA-recommended essential tools and the Microsoft Cloud Security Benchmark for data protection are based on the concept of Zero Trust (ZT). It is a security model that assumes no implicit trust and requires continuous verification of users, devices, and applications before granting access to resources. ZT applies principles such as least privilege and need-to-know, ensuring that access to data is limited to authorised entities and based on a risk-based approach. The three main principles of ZT — verifying explicitly, using least-privilege access, and assuming breach — ensure that only authorised users and devices can access resources. This goal becomes clear when the approaches of CSA and Microsoft are described in the following sections. (CSA, 2024c, p. 51; Microsoft, 2025, April 23).

5.1 Cloud data security tools

This section examines the key data security tools that are fundamental to protecting data in the cloud throughout its lifecycle, as explained by the CSA (2024c). These tools help reduce the risk of unauthorised access and data breaches, while supporting compliance and data governance. Table 5 summarises the security tool categories with brief explanations. (CSA, 2024c, pp. 213-214)

Table 5. The essential tools to secure the data lifecycle, adapted from the CSA (CSA, 2024c, pp. 213-214).

Category	Description
Identity and Access Management (IAM)	Regulates access to specific cloud resources, differentiating from general access controls, especially in IaaS and PaaS.
Access Policies	Define permissions and actions for resources, along with network rules to control traffic flow between resources.
Encryption and Key Management	Protects data by converting it to an unreadable ciphertext, with key management systems ensuring the secure handling of keys.
Masking	Replaces sensitive data with fictitious or partially obscured values, maintaining format and length, e.g., showing the last four digits of a credit card.
Tokenisation	Replaces sensitive data with unique identifiers (tokens), ensuring security and referential integrity through a separate token database.
Anonymisation	Removes personally identifiable information (PII) from data, making it irreversible and untraceable to individuals.
Data Loss Prevention (DLP)	Enforces policies to protect sensitive data, preventing unauthorised sharing or exfiltration, and ensuring data security.
Data Security Posture Management (DSPM)	Continuously assesses, monitors, and improves the security posture of cloud data, enabling proactive risk management.

Table 5 summarises the main categories of security tools that support data confidentiality, integrity, and availability in the cloud (CSA, 2024c, pp. 213-214). The following subsections describe these tools, including identity and access management, encryption, data masking, tokenisation, anonymisation, data loss prevention, and data security posture management. The section also highlights the need for continuous adaptation to new security threats and technologies.

5.1.1 Identity and access management, access policies, and encryption strategies

This section will explore mechanisms for securing cloud environments, including Identity and Access Management (IAM), access policies, and encryption techniques. IAM is crucial for cloud data security, as it governs how users and systems access specific cloud resources. It controls who can access what, when, and how, and is fundamental in preventing unauthorised access to cloud-based data. (CSA, 2024c, p. 105)

Access policies, on the other hand, define what actions authorised users or systems can perform on cloud resources. They specify permissions such as read, write, delete, or execute, and may also include network-level rules that control how data flows between resources. These rules help ensure that only authorised communication occurs within the cloud environment. (CSA, 2024c, p. 108)

For instance, in Microsoft Azure, IAM is typically implemented through RBAC, which allows administrators to assign specific roles with defined permissions to users or groups, for example, granting read-only access to a storage account. Additionally, some Azure services support separate access policies that define more granular permissions. These policies can be used to grant one group read and modify access to specific files while restricting another group to read-only access, preventing unauthorised changes or deletions. (Microsoft, 2025, March 13)

Encryption is a technique that is used to secure data by transforming it into an unreadable ciphertext. Encryption aims to ensure that only authorised users, who have the appropriate decryption keys, can access the data. In cloud environments, encryption is applied to both data at rest and in transit to prevent unauthorised access. Key management systems (KMS) are central to the effectiveness of encryption, as they store and manage the cryptographic keys for data decryption. (CSA, 2024c, pp. 216-219)

In cloud environments, encryption can be managed in different ways, depending on the organisation's specific needs. Customers may encrypt their data before storage, with keys managed separately from the CSP in a model known as client-side encryption. Alternatively, keys can be managed by the customer but provided to the CSP at runtime for server-side encryption. Another option is the Bring Your Own Key (BYOK) model, where encryption keys are managed by the CSP but are controlled by the customer. A comprehensive risk assessment is essential for determining the most suitable encryption approach. (CSA, 2024c, pp. 216-219)

Mohammad & Hussein (2023) explain that symmetric-key cryptography uses a single shared key for both encryption and decryption, while asymmetric-key cryptography employs a pair of keys: a public key for encryption and a private key for decryption. Symmetric-key cryptography is typically considered faster. However, it requires secure key distribution, while asymmetric-key cryptography provides enhanced security without the

need to share keys. Additionally, hash functions are essentiall to maintaining data integrity by generating a fixed-size output, or digest, from input data. This ensures that any alterations to the data can be detected, without revealing the original data itself. (Mohammed & Hussein, 2023, p. 4)

5.1.2 Masking, tokenisation, and anonymisation

This section will examine three key data protection techniques: masking, tokenisation, and anonymisation. Data masking is a technique that substitutes sensitive data with fictitious or partially obscured values. This allows organisations to utilise data that appears realistic for purposes such as testing or development, without disclosing actual sensitive information. For example, only the final four digits of a credit card number may be revealed, while the remaining digits are concealed. (CSA, 2024c, p. 214)

Tokenisation, on the other hand, replaces sensitive data with unique identifiers, called tokens, which are stored in a separate database. The token can be mapped back to the original data when necessary, but it does not provide direct access to the sensitive information. (CSA, 2024c, p. 214)

Anonymisation involves removing personally identifiable information from data sets, making it impossible to trace the data back to any individual. This process is typically irreversible, ensuring that once data has been anonymised, it cannot be reconstructed. (CSA, 2024c, p. 214).

In summary, masking, tokenisation, and anonymisation are techniques used to protect sensitive data in cloud environments. These methods help reduce the risk of data exposure.

5.1.3 Data loss prevention and data security posture management

This section will discuss advanced approaches to protecting sensitive data in cloud environments, focusing on Data Loss Prevention (DLP) and Data Security Posture Management (DSPM) systems. DLP systems are designed to identify, classify, and monitor sensitive data. They also ensure that this data is not shared inappropriately, either

internally or externally. For example, a DLP system might prevent the emailing of sensitive data or uploading it to an unsecured external system. (CSA, 2024c, p. 221)

Data Security Posture Management (DSPM) is an emerging category of tools specifically designed to ensure the security of data within cloud environments. While Cloud Security Posture Management (CSPM) focuses on the security of cloud infrastructure and addresses the security of cloud-based software, DSPM centres on the protection of data itself. This includes processes such as data discovery and classification, and may incorporate DLP features to assist organisations in identifying the locations of their data and evaluating its sensitivity. DSPM tools also assess overlapping access controls to determine who has access to the data. A key challenge in cloud data security is managing the various controls, often spread across different systems, which may fail to offer a unified view of data use and exposure. DSPM is designed to try and address this gap. (CSA, 2024c, p. 222)

5.2 Microsoft data protection

This section outlines Microsoft's approach to data protection in the cloud, as defined in the Microsoft Cloud Security Benchmark (MCSB) (2025). Microsoft’s data protection strategies, as outlined in the MCSB (2025), offer a framework for securing sensitive data across cloud environments. Microsoft includes built-in tools designed to support data protection in the cloud. These tools help secure data when it is stored, being transferred, or accessed. Table 6 outlines Microsoft's data protection strategies as detailed in the MCSB. (Microsoft, 2025, April 23)

Table 6. Adapted summary of Microsoft’s data protection strategies, aligned with NIST security principles, as presented in the Microsoft Cloud Security Benchmark: Data Protection (Microsoft, 2025, April 23).

Data Protection Strategy	NIST Security Principle	Description
DP-1: Discover, classify, and label sensitive data	Data Classification and Labelling	Establish and maintain an inventory of sensitive data using tools such as Microsoft Purview, Azure Information Protection, and Azure SQL Data Discovery and Classification.
DP-2: Monitor anomalies and threats targeting sensitive data	Threat and Anomaly Monitoring	Monitor for unusual activities around sensitive data, such as unauthorised transfers, using solutions like Azure Information Protection and Microsoft Defender for Storage and SQL.
DP-3: Encrypt sensitive data in transit	Data Protection in Transit	Protect data in transit using encryption protocols, such as TLS v1.2 or higher, in services like Azure Storage, and enforce secure transfer in Azure services.
DP-4: Enable data at rest encryption by default	Data Protection at Rest	Ensure data at rest is protected using encryption, with many Azure services enabling data-at-rest encryption.
DP-5: Use the customer-managed key option in data-at-rest encryption when required	Customer-Controlled Key Management	Implement customer-managed keys for encryption at rest to comply with regulatory requirements, using Azure Key Vault.
DP-6: Use a secure key management process	Secure Key Management	Document and implement a cryptographic key management standard, using Azure Key Vault.
DP-7: Use a secure certificate management process	Certificate Management	Manage the lifecycle of certificates, including creation, rotation, and revocation, using Azure Key Vault.
DP-8: Ensure the security of the key and certificate repository	Secure Key and Certificate Repositories	Secure the key and certificate repository by using Azure Key Vault.

Table 6 connects each strategy to the relevant NIST security principle and describes the tools and processes used to secure sensitive data within Microsoft. The strategies encompass critical areas, including data classification, anomaly detection, encryption, key management, and certificate management. (Microsoft, 2025, April 23)

Microsoft (2025) provides tools such as Microsoft Purview, which assist in classifying and labelling sensitive data. Monitoring anomalies, such as unusual access patterns or potential data exfiltration, can help detect and mitigate security breaches. Microsoft offers solutions like Azure Defender for SQL and Microsoft Defender for Storage, which monitor anomalies and alert users to potential threats related to sensitive data. Microsoft (2025) mandates the use of encryption protocols, such as Transport Layer Security (TLS) v1.2 or higher, to protect data transferred over public networks. Likewise, data stored in cloud services must be encrypted to prevent unauthorised access. Microsoft enables data-at-rest encryption by default in Azure services through service-managed keys. (Microsoft, 2025, April 23)

For organisations that need greater control over data protection, Microsoft offers the option of customer-managed keys (CMKs). These keys enable organisations to oversee the encryption key lifecycle, ensuring compliance with security and regulatory standards. Azure Key Vault supports the creation, storage, and management of these Customer Master Keys (CMKs). Microsoft Azure Key Vault supports the management of certificates, such as those needed for secure information exchange, allowing organisations to create, store, and manage them securely. Protecting key and certificate repositories is also essential for data protection. Microsoft Azure Key Vault offers security features, including managed identities, access controls, and encryption at rest, to safeguard these repositories. (Microsoft, 2025, April 23)

5.3 Chapter summary

This chapter has examined cloud data security tools and technologies, addressing the study question, "What are the main concepts of cloud data security and its management?". It began with an overview of the essential tools recommended by the CSA for securing the data lifecycle.

The importance of tools for data classification, monitoring, encryption, and key management was highlighted (CSA, 2024c, pp. 213-214). To illustrate these concepts, real-world examples from Microsoft Azure were briefly presented, demonstrating how these tools are implemented through the MCSB protection framework (Microsoft, 2025, April 23).

Microsoft’s tools align with recognised standards, but their full technical details are not always thoroughly disclosed in the documentation. This emphasises the need for

organisations to understand relevant standards for cloud data security and place some trust in the provider’s implementation.

6 Cloud data security challenges

Cloud computing offers organisations greater flexibility, scalability, and cost efficiency; however, it also introduces notable security concerns. Zhang et al. (2020) note that, unlike traditional on-premises storage, cloud environments restrict user control, increasing the potential for misuse or unauthorised access. This concern is amplified when data is intercepted over insecure networks or when cloud providers experience technical failures or human errors. A key issue is the loss of direct control over data once it is stored in the cloud, as it often moves across multiple networks that may not always be secure. These conditions complicate the protection of confidentiality, integrity, and availability—three foundational principles of cloud data security. (Zhang et al., 2020, pp. 12–14)

Aldossary and Allen (2016) further explain that confidentiality risks may arise from weak privacy settings and poor coordination between cloud service providers (CSPs), particularly in multi-cloud environments. Data integrity is threatened when information is altered or corrupted, while availability can be compromised by system outages, cyberattacks, or the lack of effective recovery mechanisms. (Aldossary & Allen, 2016, pp. 487–488)

Alghofaili et al. (2021) identify additional risks such as data breaches, data loss, and insufficient user account separation. These issues are significant in multi-tenant environments, where inadequate security controls may allow unauthorised access between users. (Alghofaili et al., 2021, pp. 11–13)

This chapter explores the primary challenges in ensuring cloud data security, as identified in recent studies. The aim is to address the research question: “What are the main challenges in cloud data security, according to recent studies?”. The findings outlined here will establish the foundation for the subsequent literature review.

6.1 CSA findings on challenges in cloud data security

This section highlights key security challenges for cloud data identified by the recent reports by the CSA, which emphasise the increased complexity from hybrid and multi-cloud environments. In fact, the CSA (2025) report indicates that 53% of organisations operate in hybrid environments, and 27% utilise multi-cloud systems, with larger organisations being more likely to implement these complex infrastructures. Literature states that with the

growing use of these systems, ensuring secure data management has become increasingly important. As organisations adopt these architectures more widely, securing data also becomes more challenging. (CSA, 2022, p. 7; CSA, 2024b, p. 26; CSA, 2025, p. 7)

According to the CSA (2022b), organisations often struggle to distinguish between sensitive and non-sensitive data, resulting in either insufficient protection for sensitive data or unnecessary expenditure on excessive security measures (CSA, 2022b, p. 11). Another CSA (2025) survey reports similar findings, indicating that many organisations struggle to identify their sensitive data (CSA, 2025, p.6). A high proportion of respondents reported low confidence in their ability to locate the organisation's sensitive data, an issue that is made worse by the use of hybrid and multi-cloud environments (CSA, 2025, p.6).

Weak access controls in IAM systems expose organisations to significant risks, making it more challenging to ensure that only authorised individuals can access specific resources (CSA, 2024b, p. 14). Misconfiguration, inadequate monitoring, and outdated systems can create vulnerabilities in IAM (CSA, 2024b, p. 14). Many organisations also lack effective logging and monitoring systems, leading to undetected data breaches and significant damage (CSA, 2024b, pp. 11–12).

The risk increases when data is shared with third parties, such as vendors and contractors. CSA’s 2022 report indicates that over 80% of organisations are concerned about data loss when dealing with third parties, primarily due to a lack of control over how external partners manage and secure data. (CSA, 2022a, p. 7; CSA, 2022b, p. 12)

Furthermore, technical challenges, staff shortages, and low automation levels hinder cloud security improvements, with 48% of survey respondents citing limited personnel and 46% highlighting inadequate automation as barriers to enhancing data security (CSA, 2025, p. 9). Although regulatory compliance remains the primary reason organisations invest in data security, CSA emphasises that a broader risk management approach is needed to address the diverse threats facing cloud environments (CSA, 2025, pp. 12–13).

Fragmented security tools also contribute to these challenges, as 54% of organisations report using four or more tools to manage data risks, and 26% state that poor integration makes their security management more difficult (CSA, 2025, p. 10). Many continue to rely

on traditional security tools designed for on-premises systems, which are not well-suited for integration with hybrid and multi-cloud environments, thereby limiting visibility and hindering effective risk management (CSA, 2025, p. 8). Notably, 54% of organisations depend on four or more tools for managing data security, and 26% identify poor integration as a key challenge (CSA, 2025, p. 8). Tools such as data loss prevention, threat detection, and encryption are commonly employed, and they often lack the necessary coordination to secure distributed cloud systems, particularly within hybrid and multi-cloud contexts (CSA, 2025, p. 9). In response, some organisations are adopting more integrated security solutions, incorporating features such as risk scoring, visual dashboards, and structured risk assessments (CSA, 2025, p. 10).

To summarise, the CSA highlights several significant challenges in cloud data security, particularly as organisations increasingly adopt hybrid and multi-cloud environments (CSA, 2022a, p. 7; CSA, 2024b, p. 26). While regulatory compliance drives much of the investment in data security, a broader risk management approach is crucial to address the evolving threats faced by organisations (CSA, 2025, pp. 12–13).

6.2 Cloud data security considerations in emerging technologies

This section briefly examines how emerging technologies—specifically AI, quantum computing, and the Internet of Things (IoT)—introduce new considerations for cloud data security. Although these technologies are not the primary focus of this thesis, they are closely linked to cloud data security, and understanding them provides valuable context for reviewing recent research on the subject. In an article published by the CSA, Chaudhary (2024) acknowledges that emerging technologies such as AI, quantum computing, and the IoT introduce new security challenges and increase the attack surface, necessitating stronger protection measures (Chaudhary, 2024). The following paragraphs offer brief definitions of these three technologies.

The CSA Quantum-Safe Security Working Group states that quantum computing poses a threat to encryption methods, as quantum algorithms could potentially compromise existing cryptographic systems. The absence of quantum-resistant algorithms, combined with the emerging development of quantum computing, creates security vulnerabilities that require attention. Nonetheless, quantum computing also offers opportunities, such as the

development of new, stronger cryptographic methods to secure cloud data in the future. (Missimore, 2025)

The CSA AI Organisational Responsibilities report (2024d) highlights the strong connection between AI and cloud data security. It outlines the necessity for organisations to adopt clear practices to protect data, AI models, and the AI development process. The report introduces the AI Shared Responsibility Model, which divides security tasks between service providers, application owners, developers, and users. Key concerns include managing data, preventing harmful inputs, and ensuring user accountability. Additionally, the report emphasises the significance of data privacy in AI training, concentrating on data authenticity, anonymisation, and secure access while complying with regulations such as the GDPR. (CSA, 2024d, pp. 7-10, 19-21)

The CSA (2024e) report on Zero Trust for IoT recommends employing Zero Trust (ZT) principles to tackle security risks in IoT environments (CSA, 2024e, pp. 6-9). As explained earlier in the thesis, ZT assumes no trust by default, verifying every access request with rigorous identity checks and restricting access to ensure that only authorised users and devices can access sensitive data (Microsoft, June 8, 2025). The CSA report emphasises the necessity of securing cloud data in IoT systems by guaranteeing data authenticity, anonymisation, and secure transmission, thereby protecting the confidentiality, integrity, and availability of data as IoT risks evolve. (CSA, 2024e, pp. 6-9)

In conclusion, this section highlights the significant influence of emerging technologies—namely AI, quantum computing, and the IoT—on cloud data security. Although these technologies introduce new vulnerabilities, they also offer opportunities to strengthen data protection through advanced security methods. (CSA, 2024d, pp. 7–10, 19–21; CSA, 2024e, pp. 6–9; Missimore, 2025)

6.3 Securing cloud databases

This section examines challenges in securing cloud-based databases, focusing on the risks to data both at rest and during transmission, as discussed in a review by Ibqal et al. (2024). It emphasises the technical vulnerabilities and organisational constraints that make it harder to protect data in the cloud setting adequately. (Ibqal et al., 2024, pp.12-19)

Iqbal et al. (2024) review the challenges in securing cloud-based databases, focusing on threats to data both at rest and in transit. They identify weak authentication systems, attacks such as man-in-the-middle, and risks including data leakage, hijacking, and unauthorised modifications to data at rest as significant concerns for maintaining data confidentiality, integrity, and availability. (Ibqal et al., 2024, pp.12–19)

Issues include inadequate access control, insider misuse, and ambiguous data definitions. The review identifies vulnerabilities that arise from both internal sources, such as human error or malicious actions, and external sources, including attacks that exploit weaknesses in systems and networks. In shared environments, poor security practices by one user can jeopardise the security of others. The lack of security measures at lower levels, such as the network or operating system, facilitates attackers in bypassing higher-level defences. (Iqbal et al., 2024, pp. 15–16)

The review also mentions organisational resource challenges, such as a lack of trained personnel and insufficient system maintenance. Moreover, incorrect encryption and anonymisation methods might heighten the risk of data exposure. In addition, ambiguous regulations and weak enforcement pose challenges to compliance. (Iqbal et al., 2024, pp. 17-18)

In summary, Iqbal et al.'s review highlights the numerous challenges that cloud data security faces. It advocates for stronger security measures, more efficient resource allocation, and clearer security frameworks to effectively address these risks. (Iqbal et al., 2024, pp. 12-19)

6.4 Chapter summary

The findings across the three sections of the chapter —CSA findings, Ibqal et al. review, as well as Emerging technologies — highlight common challenges in cloud data security. A key similarity is the concern regarding access control and data protection. All chapters emphasise the risks associated with weak access controls, misconfigurations, and inadequate monitoring systems (Zhang et al., 2020, pp. 12-14; Aldossary & Allen, 2016, pp. 487-488; CSA, 2022b, p. 11; CSA, 2024b, p. 14; Iqbal et al., 2024, pp. 12-19). Additionally, each chapter identifies the issue of fragmented or outdated security tools that impede

effective risk management (CSA, 2025, p. 8; CSA, 2025, p. 10; Iqbal et al., 2024, pp. 15–16).

The reviewed literature indicates that organisations face challenges in implementing effective cloud data security management. These include human factors, such as staff shortages, budget constraints and inadequate training, which are recurring issues (CSA, 2025, p. 9; Iqbal et al., 2024, pp. 17-18). Moreover, the emerging technologies discussed in the second section- AI, quantum computing, and IoT- introduce new risks but share common security concerns with traditional cloud systems, particularly regarding encryption and data privacy (Chaudhary, 2024; Missimore, 2025; CSA, 2024d, pp. 7-10, 19-21; CSA, 2024e, pp. 6-9). Furthermore, a strong focus on compliance does not always guarantee comprehensive security, suggesting that regulatory adherence alone may be insufficient to address evolving risks (CSA, 2025, pp. 12–13).

Figure 4 presents a word cloud that highlights the key challenges identified in research on cloud data security. This image was created by OpenAI (2025) to visually summarise the issues discussed in Chapter 6. The challenges mentioned in the chapter were compiled by the author into a word list and entered into ChatGPT with the prompt "Create a word cloud of the following word list."

Figure 4. Key data security challenges in cloud computing. (OpenAI, 2025)


Data Visibility
Data Classification
Access Controls
Insufficient Monitoring
Technical Failures
and Misconfigurations
Limited Budget
Skilled Staff Constra
ints
Data Definitions
and Semantics
Access Control
Misconfigurations
Compliance Focus
vs Risk Management

7 Methods

This chapter outlines the research methodology employed to conduct a systematic literature review, guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework. The review sought to answer the following research question: “What new technologies to improve cloud data security were introduced in research from January 2024 to February 2025, and what challenges do they address?” The PRISMA framework was chosen for its widely recognised capacity to ensure transparency, structure, and replicability in systematic reviews across academic disciplines (Page et al., 2021, p. 1).

The PRISMA methodology includes defining the review protocol, selecting appropriate data sources, formulating a search strategy, and establishing inclusion and exclusion criteria (Page et al., 2021, p. 5). This systematic approach contributes to the objectivity and comprehensiveness of the review process (Foroudi & Dennis, 2024, Chapter 4, Background section).

To collect relevant literature, three prominent academic databases were examined: Wiley Online Library, ACM Digital Library, and SpringerLink. These databases were selected due to their extensive coverage of topics relevant to cloud computing and data security, and the provision of peer-reviewed research publications. The search was limited to these databases to maintain a manageable scope for the review, as the author conducted the research alone as a student researcher. Grammarly, an AI-powered writing assistant, was employed to enhance language clarity and accuracy. The use of AI in this work complies with the guidelines from Hämeen Ammattikorkeakoulu (Häme University of Applied Sciences, n.d.).

The thesis acknowledges its scope and limitations and states that it does not claim to be a professional-level systematic literature review. While it examines key concepts, emerging technologies, and challenges in cloud data security, it excludes several closely related areas, such as the Internet of Things (IoT), blockchain, data security in artificial intelligence, cloud application security, health cloud security, and big data in the cloud. These topics, although relevant, fall outside the defined scope of this thesis, which also excludes other related topics.

7.1 Search strategy and study selection criteria

A search strategy identified research studies on cloud data security solutions and their challenges. Keywords such as "cloud data security," "data protection," "data privacy," "data integrity," and "data confidentiality" were combined to cover the topic. Other terms, including "data security in cloud computing" and "privacy challenges in cloud environments," were also tested. The best results were obtained by focusing on "cloud data security," which yielded a more targeted set of studies.

In systematic literature reviews (SLRs), clearly defining the inclusion and exclusion criteria ensures that the selected studies align with the research objectives. These criteria are established at an early stage, alongside the development of the search strategy. Inclusion criteria highlight the study's relevance, while exclusion criteria remove studies that fall outside the review's scope. (Foroudi & Dennis, 2024, Chapter 4, Building and Meeting the Criteria of Inclusion/Exclusion section)

The following inclusion and exclusion criteria were used for the literature search:

Inclusion Criteria

- The title or abstract includes "cloud data security" or variations (e.g., "data security in cloud environments")..
- The study addresses data security in cloud computing, focusing on challenges and solutions.
- The primary aim of the study is to enhance data security in the cloud.
- The publication is an original research article.
- Published between January 2024 and February 2025.
- Written in English and available in full text.
- Peer-reviewed

Exclusion Criteria

- Studies that address cloud data without concentrating specifically on security aspects.
- Studies that do not analyse data-level security in cloud infrastructure.
- Studies addressing cloud data security in a broader or unrelated context, lacking direct relevance to data-level security.

- Case studies.
- Systematic literature reviews, general review articles, and conference papers.
- Survey-based research.
- Research focuses on health cloud, IoT computing, big data cloud, the internet of everything, and quantum computing.

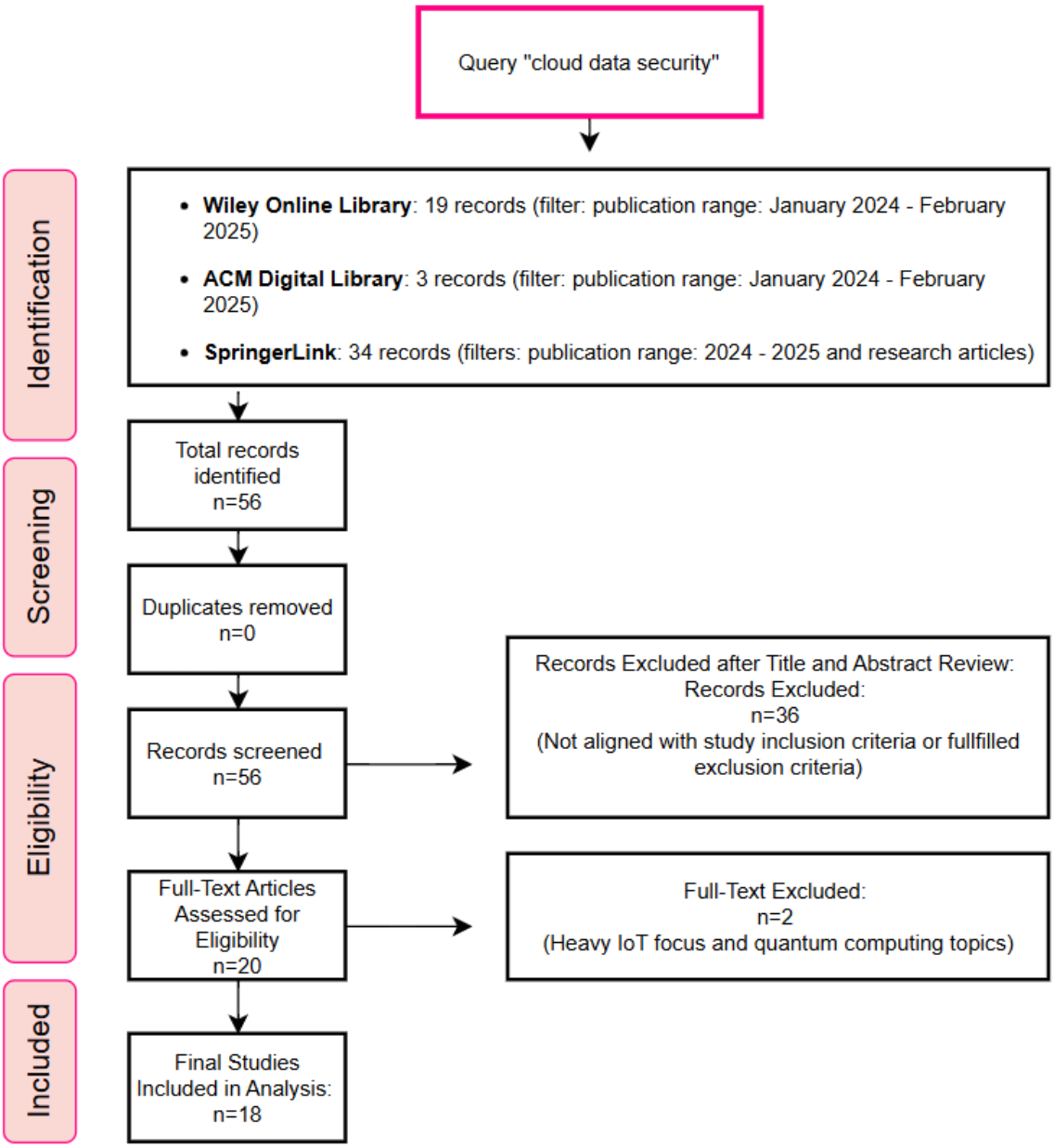
7.2 Selection process

In line with PRISMA guidelines, the review followed a systematic approach. Initially, duplicate studies were eliminated, and a manual assessment of titles and abstracts was carried out to determine relevance. This screening was conducted by one student researcher, which may have restricted the variety of perspectives. The goal of this phase was to include only pertinent studies while excluding those that were not relevant. (Page et al., 2021, pp. 4-6)

The subsequent step entailed downloading complete PDF versions of chosen studies. As indicated by Foroudi and Dennis (2024), this stage necessitates thorough reading to verify their relevance. Two studies, which initially seemed relevant based on their titles and abstracts, were ultimately discarded because one concentrated primarily on IoT while the other focused on quantum computing, both of which were criteria for exclusion. These studies were designated as "full-text excluded" per PRISMA guidelines. The search records and citations were managed with Zotero. In conclusion, the full texts of the selected studies were reassessed to ensure they adhered to the established inclusion criteria. (Foroudi & Dennis, 2024, Chapter 4, Screening Phase: Nvivo and Bibliometrix section; Page et al., 2021, pp. 4-6)

The literature search was conducted on 23 February 2025, using the search term "cloud data security" across three primary databases: Wiley Online Library, ACM Digital Library, and SpringerLink. The PRISMA flow diagram (Figure 4) was adapted to guide the systematic review process.

Figure 4 . Flow diagram illustrating the systematic review process, showing the steps taken to identify and select relevant studies for the review.



The initial search identified 56 studies: 19 from the Wiley Online Library, three from the ACM Digital Library, and 34 from SpringerLink. The search filters applied included a publication range from January 2024 to February 2025 for both the Wiley Online Library and the ACM Digital Library. For SpringerLink, the same publication range was applied, along with a filter for "research articles."

There were no duplicate studies across the three databases, resulting in a total of 56 unique studies. A review of the titles and abstracts resulted in the exclusion of 36 studies that did not align with the selection criteria, leaving 20 studies for full-text analysis.

Upon reviewing the complete texts, two studies were excluded: one concentrated significantly on the Internet of Things (IoT), while the other was primarily centred on quantum computing. Consequently, 18 studies were included in the final analysis.

7.3 Synthesis and empirical validation of the selected studies

This section provides a synthesis of the 18 studies included in the analysis. The key data from each study has been organised in Table 7, which lists the authors, the primary security challenges addressed, and the technologies or methods proposed to enhance cloud data security. The relevant information was extracted by one researcher, drawing the information from each study's abstract, introduction, methods, results and conclusion sections.

Table 7. Cloud data security challenges and solutions in selected studies.

Authors	Name of the study	The main cloud data security challenge addressed	Cloud data security technology/methodology introduced
Akhtar et al., 2024	Inter-Cloud Data Security Framework to Build Trust Based on Compliance with Controls	Ensuring data security and trust among CSPs in an inter-cloud environment	The FBI-TDS framework offers controls to mitigate data threats and establish trust among CSPs. It features a Data Security Compliance Monitor for ongoing compliance checks and assessments of trustworthiness.
Alandjani, 2024	A novel hybrid dwarf-based Archimedes optimization (HDAO) algorithm for preserving secure data in a cloud computing environment	Addressing data breaches, loss of confidentiality, and insufficient control in cloud environments	Introduces the HDAO algorithm for key generation in a three-layered framework (sanitisation, key generation, restoration) to enhance data privacy and integrity.
Bandyopadhyay et al., 2024	Parallel BFS through pennant data structure with reducer hyper-object based data hiding for 3D mesh images	Overcoming limitations of existing 3D image steganography techniques	Introduces a 3D image steganography method using Parallel BFS and a 'bag' data structure for improved embedding capacity, speed, and attack resilience.

Bansal et al., 2025	An efficient strategy for ensuring multi-cloud information security	User data security in multi-cloud environments: Preventing unauthorised access to user data, addressing issues like server collusion and CSP compromise.	Two-Fish 256-integrative symmetric key cryptography utilises a hybrid algorithm that combines AES and Two-Fish to secure user data. The data is segmented, encrypted, and distributed across multiple... CSPs, ensuring no single CSP has full access to the data.
Bhattacharjee et al., 2024	Leveraging chaos for enhancing encryption and compression in large cloud data transfers	Addressing privacy, integrity, and efficiency challenges in cloud data transfers	Proposes a chaos-based compression and encryption system using a chaotic S-box and adaptive Huffman encoding for better efficiency.
Jasmine et al., 2025	An efficient secure cryptosystem using improved identity-based encryption with multimodal biometric authentication and authorisation in cloud environments	Addressing data breaches and unauthorised access through improved authentication and encryption	Proposes SMCAAS, integrating identity-based encryption, biometrics, cryptographic hashing, and lightweight cyphers to enhance cloud data security and scalability.
Jose et al., 2024	A multi-objective privacy preservation model for cloud security using hunter prey optimization algorithm	Addressing persistent risks to sensitive cloud-stored data	MOPP-CS-HPOA combines data sanitisation, key generation, and multi-objective optimisation via HPOA to enhance privacy and utility in cloud environments.
Ma et al., 2024	Layered quantum secret sharing scheme for private data in cloud environment system	Protecting private data from unauthorised access, internal threats, and breaches	Introduces a secret sharing scheme via multi-particle entanglement and the BB84 protocol to securely distribute data across cloud servers, ensuring confidentiality.
Mohammed et al., 2024	PRC6: Hybrid lightweight cipher for enhanced cloud data security in a parallel environment	Securing cloud data transmission efficiently in limited computational resources	Introduces PRC6, a hybrid cipher of modified RC6 and Cha-cha, optimized for parallel processing to enhance cloud data security.

Nidhya et al., 2025	Optimising security and quality of service in a multi-cloud platform using a novel approach	Malicious traffic detection and Quality of Service (QoS) management in multi-cloud environments, particularly during cyberattacks like DoS.	Integrated Ant Lion Optimised Boosted Gated Recurrent Unit - A novel method that combines ant-lion optimisation with boosted gated recurrent units to enhance malicious traffic detection and quality of service management in multi-cloud platforms.
Pradhan, G., et al., 2024	A trusted computing framework for cloud data security using role-based access and pattern recognition	Preventing unauthorised access and detecting malicious activities in cloud environments	Presents the Secure Framework through Behaviour and Role Analysis, a system that assesses user trust and identifies attacks in real time, thereby improving security for cloud data access.
Rani et al., 2024	SDESA: Secure cloud computing with gradient deep belief network and congruential advanced encryption	Enhancing data confidentiality and integrity during transmission and storage	Introduces the Stochastic Deep Encryption Standard Algorithm (SDESA), which combines user authentication and data encryption to ensure the security of cloud data during both transmission and storage.
Ranjan et al., 2024	Advancing multi-cloud: an efficient crypto strategy for securing unstructured information distribution	Securing unstructured cloud data in multi-cloud environments	Proposes an effective cryptographic strategy to secure the distribution of unstructured data in multi-cloud environments.
Srivastava, A. K., et al., 2024	An Enhanced D Level Cut-Off Point-Quantum Secret Sharing Access Structure Scheme Based Efficient Monitoring Key Ciphertext Attributes	Addressing unauthorised access, ineffective key updates, and a lack of user monitoring in cloud environments	Introduces the EdLCp-QSS framework, which integrates MKCABE, blockchain, and a key control mechanism to enhance cloud data security, ensuring continuous monitoring and key updates.
Tiwari & Jha, 2024a	THC-DFECC-based privacy preserved smart contract creation for cloud data security	Addressing data security, unauthorised access, and secure data transfer in cloud environments	Introduces a Smart Contract framework utilising Twisted Hessian Curve-based Digit Folding Elliptic Curve Cryptography for data security, Gini Canberra-k-anonymity for privacy, and Exponential Entropy-based SWIFFT hashing for integrity. Data is uploaded to IPFS and verified through blockchain, ensuring

			decentralised, immutable storage.
Tiwari & Jha, 2024b	An efficient signed SSL/TLS-based data security in the cloud using LTT-DDBM and RSASK-TECC	Addressing multiple cloud security attacks (SSL/TLS Renegotiation Attack, SSL/TLS Downgrade Attack, SSL/TLS Hijacking Attack, Sweet 32 Attack) and insecure communication between cloud servers and browsers	This framework introduces a security system that employs Signed SSL/TLS, LTT-DDBM for detecting attacks, and RSASK-TECC for encrypting session keys to strengthen cloud data security. It utilises REKL-Streebog hashing for improved authentication and validation.
Yang, C., et al., 2024	Block-based fine-grained and publicly verifiable data deletion for cloud storage	Ensuring secure and efficient data deletion	Introduces a vector commitment-based method for fine-grained, publicly verifiable data deletion that allows for block-level deletion and public verification.
Zhou et al., 2024	A lattice-based searchable encryption scheme with multi-user authorisation for the certificateless cloud computing environment	Addressing vulnerabilities in public key encryption with keyword search	Introduces a lattice-based searchable encryption scheme with certificateless authentication and proxy re-encryption to enhance security against keyword guessing attacks.

During the review of the selected studies for this literature review, it became apparent that all the technologies underwent varying degrees of quantitative empirical testing. Empirical testing is essential for validating the suggested solutions (George, 2024). For instance, Akhtar et al. (2024) and Bansal et al. (2025) conducted experiments to evaluate their proposed frameworks, demonstrating that they enhance cloud data security (Akhtar et al., 2024, p. 18; Bansal et al., 2025, p. 47). Likewise, other studies, including Alandjani (2024) and Ranjan et al. (2024), evaluated their algorithms for performance efficiency, examining metrics such as encryption and decryption times (Alandjani et al., 2024, p. 128; Ranjan et al., 2024, p.143).

This thesis does not include specific details of the testing methods, such as the tools used. The scope of this thesis was to focus on solutions for enhancing cloud data security and the challenges they address, rather than to provide an analysis of empirical testing

methods. The potential validity constraints arising from the empirical testing methods will be briefly discussed in Section 9.4 of the thesis.

8 Results

This chapter presents the findings from the 18 empirical studies reviewed in this thesis, addressing the primary research question: “What new technologies have improved cloud data security from January 2024 to February 2025, and how do they address existing challenges?”. The findings are categorised into five thematic areas: encryption and cryptographic techniques, access control and authentication, data integrity and privacy, inter-cloud security, and multi-cloud security.

Firstly, an overview of the results is presented, summarising the key challenges identified in the studies and the innovative solutions to overcome them. Then, the five identified thematic areas are explored in detail.

8.1 Overview of the results

The 18 studies included in this systematic review offer cloud data security solutions that have been empirically and quantitatively tested. The primary challenges and solutions identified in the selected studies, covering various aspects of cloud data security, are summarised in Table 8.

Table 8. A simplified list of the main challenges and corresponding solutions extracted from the 18 selected studies.

Challenges in cloud data security		Cloud data security solutions
Inter-cloud security and trust	→	Trust and compliance monitoring
Data breaches and confidentiality	→	Key generation and privacy
Image protection limitations	→	Image data protection
Multi-cloud user data security	→	Hybrid encryption
Data transfer privacy	→	Enhancing privacy in data transfer
User authentication	→	Biometric authentication
Data transmission security	→	Secure data transmission
Malicious traffic	→	Malicious traffic detection
Access control	→	Real-time access security, key updates, and continuous monitoring
Data confidentiality and integrity	→	User authentication and data encryption
Securing unstructured data	→	Unstructured data security
Insecure communication and attacks	→	Session encryption and attack detection
Efficient data deletion	→	Data deletion verification
Keyword guessing attacks	→	Improved authentication and data encryption

Table 8 illustrates how existing research aims to solve challenges in cloud data security by developing new technologies and solutions. These encompass solutions such as trust monitoring, encryption methods, enhanced user authentication, malicious traffic detection, and optimised transmission techniques. The challenges addressed include, for example, access control, data confidentiality and integrity, inter-cloud security, data breaches, and insecure data transfer. The relevant information was extracted by one student researcher, drawing the information from Table 7, which listed the authors, the primary security challenges addressed, and the technologies or methods proposed to enhance cloud data security in the 18 selected studies.

The 18 studies for the systematic review are categorised into thematic areas in Table 9, based on their primary focus.

Table 9. Categorisation of the selected 18 studies on cloud data security into five thematic categories of cloud data security.

Encryption and cryptographic techniques (n=9)	Access control and authentication (n=3)	Data integrity and privacy (n=4)	Inter-cloud data security (n=1)	Multi-cloud data security (n=1)
Alandjani et al., 2024	Jasmine et al., 2025	Bandyopadhyay et al., 2024	Akhtar et al., 2024	Nidhya et al. 2025
Bansal et al., 2025	Pradhan et al., 2024	Jose et al., 2024		
Bhattacharjee et al., 2024	Srivastava et al., 2024	Ma et al., 2024		
Mohammed et al., 2024		Yang et al., 2024		
Rani et al., 2024				
Ranjan et al., 2024				
Tiwari & Jha, 2024a				
Tiwari & Jha, 2024b				
Zhou et al., 2024				

Table 9 was compiled by one student researcher, who aimed to identify common themes across the studies. Although some studies could fit into more than one category, the analysis concentrates only on what the researcher regarded as the main security solution. This assessment may be subjective and limited. The researcher employed a systematic method, based on the information in Table 7. That table was created by reviewing the abstract, introduction, methods, results, and conclusion of each study to find recurring

themes and determine the primary focus. The categories in Table 9 are therefore derived from the data in Table 7.

The first thematic category, encryption and cryptographic techniques, highlights advancements in encryption algorithms and key management (Alandjani et al., 2024; Bansal et al., 2025; Bhattacharjee et al., 2024; Mohammed et al., 2024; Rani et al., 2024; Ranjan et al., 2024; Tiwari & Jha, 2024a, 2024b). The second category, access control and authentication, focuses on enhancing methods for verifying user identities and managing access to sensitive cloud data (Jasmine et al., 2025; Pradhan et al., 2024; Srivastava et al., 2024). The third thematic category, data integrity and privacy, entails technologies that protect the integrity of cloud data, ensuring it remains secure and confidential (Bandyopadhyay et al., 2024; Jose et al., 2024; Ma et al., 2024; Yang et al., 2024). Inter-cloud security highlights the importance of trust and safety among different cloud service providers, focusing on compliance, monitoring, and the secure sharing of data (Akhtar et al., 2024). The last category, multi-cloud security, addresses the complexities of safeguarding data across multiple cloud platforms (Nidhya et al., 2025). The following sections examine each thematic area in detail.

8.2 Encryption and cryptographic techniques

This section describes the nine studies in the thematic category of encryption and cryptographic techniques. Mohammed et al. (2024) suggest a hybrid encryption method that merges block and stream cyphers, providing stronger security and improved resistance to attacks, while ensuring efficient data protection in the cloud (Mohammed et al., 2024, p. 105). Bansal et al. (2025) explore AES and Twofish algorithms in multi-cloud environments, emphasising their role in securing data both during storage and during transfer, as well as in managing encryption keys efficiently (Bansal et al., 2025, p. 47). Alandjani et al. (2024) introduce a novel key generation method designed to enhance data privacy and integrity (Alandjani et al., 2024, p. 128).

Tiwari and Jha (2024a) propose an intelligent contract system utilising elliptic curve cryptography to ensure data privacy and secure access control (Tiwari & Jha, 2024a, p. 163). Rani et al. (2024) introduce a deep learning-based encryption method that enhances data confidentiality and integrity (Rani et al., 2024, p. 118). Ranjan et al. (2024) propose a combined encryption technique to enhance the security of unstructured data in multi-cloud

environments (Ranjan et al., 2024, p.143). Bhattacharjee et al. (2024) focus on improving data privacy and minimising information loss during large-scale cloud data migrations (Bhattacharjee et al., 2024, p. 250). Tiwari and Jha (2024b) introduce a security framework using secure transmission protocols and advanced cryptographic methods (Tiwari & Jha, 2024b, p. 178). Zhou et al. (2024) propose a searchable encryption method to protect cloud data from keyword guessing attacks (Zhou et al., 2024, p.195). These nine studies emphasise the importance of encryption and cryptographic techniques in protecting cloud data.

8.3 Access control and authentication

This section describes the three studies in the thematic category of access control and authentication techniques. The studies enhance user verification and regulate access to cloud resources. Pradhan et al. (2024) propose a security framework that monitors user behaviour and roles (Pradhan et al., 2024, p. 220). Srivastava et al. (2024) introduce a system that combines advanced encryption and blockchain technology to control data access (Srivastava et al., 2024, p. 228).

Jasmine et al. (2025) present a framework that integrates biometric authentication with advanced encryption, verifying user identity through multiple biometric features, such as fingerprint and iris recognition (Jasmine et al., 2025, p. 545). The three studies in this category illustrate the development of access control and authentication methods in cloud environments.

8.4 Data integrity and privacy

This section describes the four studies in the thematic category of data integrity and privacy techniques. The studies focus on protecting the integrity, privacy, and availability of data in cloud environments. Bandyopadhyay et al. (2024) present a method for securely concealing sensitive data within 3D image files, thereby reducing the risk of unauthorised access (Bandyopadhyay et al., 2024, p. 250).

Yang et al. (2024) propose a secure data deletion method that allows users to remove data parts in a verifiable manner (Yang et al., 2024, p. 118). Ma et al. (2024) introduce a system

that segments confidential data and stores it separately, thereby complicating access for unauthorised users (Ma et al., 2024, p. 380). Jose et al. (2024) emphasise the protection of private information while ensuring its usability through data restoration and secure access keys (Jose et al., 2024, p. 213).

8.5 Inter-cloud and multi-cloud security

This section describes the two studies in the thematic categories of inter-cloud and multi-cloud security. Inter-cloud security helps build trust between CSPs. Akhtar et al. (2024) propose a framework that requires CSPs to follow security rules and regularly check their compliance. This framework includes a system for assessing each provider's security, aiding in better collaboration. The FBI-TDS framework also offers Data Trust as a Service (DTaaS), which evaluates CSP trustworthiness through compliance checks, user feedback, and security audits. (Akhtar et al., 2024, p.18)

The second study highlights the challenges and solutions associated with securing data across multiple CSPs in multi-cloud environments. Nidhya et al. (2025) propose an intelligent system that enhances the detection of malicious traffic and ensures reliable service delivery during cyberattacks on a multi-cloud platform. The proposed system achieves high accuracy in detecting malicious traffic while maintaining service quality with minimal violations. (Nidhya et al., 2025, p. 9)

8.6 Chapter summary

This chapter presented the findings from the 18 selected studies on cloud data security, addressing the research question “What new technologies improved cloud data security from January 2024 to February 2025, and how did they address existing challenges?”.The studies were categorised into five thematic areas: encryption and cryptographic techniques, access control and authentication, data integrity and privacy, inter-cloud security, and multi-cloud security.

The thematic areas covered included developments in encryption and cryptography, with a focus on hybrid systems and key generation. Also, access control methods using biometric authentication and role-based systems were presented. Techniques for data integrity and

privacy, such as data splitting and secure data deletion, were addressed. Security frameworks for trust and compliance between cloud providers, as well as the challenges of securing data across multiple clouds, were also covered.

9 Discussion

This chapter presents a discussion of the thesis's findings, exploring the main concepts, challenges, and technological advancements in cloud data security. The discussion is structured to cover the three research questions (1) “What are the main concepts of cloud data security and its management?” (2) “What are the main challenges in cloud data security, according to recent research?” (3) “What new technologies to improve cloud data security were introduced in research from January 2024 to February 2025, and what challenges do they address?”.

The chapter begins with a discussion of fundamental cloud data security concepts, including key services and security frameworks. It then examines the main challenges faced by organisations and concludes by exploring new security technologies such as encryption, access control, and data integrity, along with the challenges they aim to address. All of this is written reflecting on the theoretical background of the thesis.

In addition to answering the research questions, this chapter reflects on the practical implications of the findings, identifies gaps in the research, and considers the ethical aspects and limitations of the thesis.

9.1 Main concepts of cloud data security and its management

Chapters 2 to 5 aimed to answer the research question “What are the main concepts of cloud data security and its management?”. The chapters provided an exploration of cloud services, data protection methods, and the secure data lifecycle, offering an understanding of how cloud data security can be managed. Key concepts of cloud computing were distinguished from traditional IT models, providing insight into cloud infrastructure (NIST, 2011, p. 2; AWS, 2025; Microsoft, 2025b). The main service and deployment models were examined, emphasising how responsibilities shift depending on the chosen model (CISA, 2022, p. 5; Microsoft, 2024, September 26). Furthermore, multi-cloud strategies were briefly described, highlighting the complexities and additional management requirements organisations face when increasingly adopting such environments (CISA, 2022, pp. 7-8; HashiCorp, 2021).

The principles of cloud data security were explored, emphasising data classification, data states, types of cloud storage, and the data lifecycle. The discussion highlighted the importance of implementing specific security measures for data at rest, in motion, and in use, as well as the critical role of accurate data classification for ensuring adequate security (CSA, 2024c, pp. 209-213; CSA, 2025, p. 210).

The chapter also highlighted the risks associated with dark data, which is a recognised challenge in organisations (CSA, 2022b, p. 15; CSA, 2025, p. 6). The concept of the data lifecycle was discussed, emphasising its importance for ensuring data security and compliance from creation to completion and disposal (CSA, 2024a, p. 6). The CSA Compliance Checklist for Data Lifecycle Management was introduced as a practical tool for aligning data governance practices with legal regulations, particularly the GDPR (CSA, 2024a, pp. 17-18). Microsoft's Cloud Security Benchmark (2025) was examined, illustrating practical strategies for securing sensitive cloud data and highlighting the need for a multi-layered security approach (Microsoft, 2025, April 23).

The role of security frameworks, including the NIST CSF and the CIA triad, was explored as a structured approach to securing cloud data (CSA, 2024a, pp. 12-15; ENISA, 2024a, p. 29; NIST, 2024, p. 10). Legal frameworks, especially the GDPR, were discussed, highlighting their important role in the regulatory landscape for cloud data security. The increasing number of EU cybersecurity laws highlights the rising demand for data protection compliance (European Commission, n.d.).

The section also discussed the importance of understanding the shared responsibility model, which divides cloud security tasks between CSPs and CSCs according to the service model. The model emphasises the need for CSCs to take an active role in securing their data. (CISA, 2022, p. 5; CSA, 2024c, pp. 21-23)

Lastly, the chapter recognised increasing concerns about the environmental impact of cloud infrastructures, emphasising the importance of sustainable cloud data governance in compliance with ESG and emerging regulations for sustainable digital practices. A rising need for innovative solutions to cut carbon emissions and resource waste was also discussed. (CSA, 2024a, p. 148; Storj, 2023, pp. 12-19)

The findings from the reviewed literature highlight the importance of fully understanding the shared responsibility of cloud data security between CSPs and CSCs. Furthermore, the findings suggest that effective protection of cloud data depends on aligning security frameworks with regulatory requirements and applying recognised best practices. Additionally, effective cloud data security management also needs to be sustainable and consider the ESG standards and regulations. The reviewed literature, however, does not present a single, comprehensive approach to cloud data security management. This suggests that organisations must interpret and apply these principles according to their specific needs, highlighting the importance of careful planning of cloud data security management. Furthermore, Microsoft's tools align with recognised standards, though technical documentation does not always disclose full implementation details, resulting in a degree of reliance on the provider's internal practices. Lastly, while the reviewed literature provides a solid foundation for understanding cloud data security principles, it does not address all the practical challenges organisations may face in applying them or fulfilling security responsibilities across service models. These issues, while significant, fall outside the scope of this thesis.

9.2 Main challenges in cloud data security

This section discusses the main cloud data security challenges highlighted in recent literature, answering the research question: "What are the main challenges in cloud data security, according to recent studies?". A key data security challenge stated in literature is decentralised data management in cloud environments, which reduces oversight and increases risks such as unauthorised access and data breaches (Zhang et al., 2020, pp. 12-14). Similarly, CSA (2022b) identified the inherent complexity of cloud infrastructures as a key challenge, particularly when organisations often lack clear visibility into how their data is managed and who has access to it (CSA, 2022b, p. 7). Iqbal et al. (2024) elaborated that in shared cloud environments, weak security practices by one user can undermine the security of others (Iqbal et al., 2024, pp. 13–14). Access control was highlighted as a central method to protect the confidentiality, integrity, and availability of cloud data (CSA, 2024b, pp. 11–12). Furthermore, the issue of data classification was recognised as crucial for maintaining cloud data confidentiality and integrity, as improper practices can lead to inadequate protection of sensitive data or unnecessary spending on the protection of non-sensitive data, wasting resources (CSA, 2022b, p. 11). Similarly, Iqbal et al. (2024)

highlighted that poorly defined access controls and unclear data definitions increase the risk of unauthorised access, exposing data to internal and external threats (Iqbal et al., 2024, pp. 13–14). This issue was found to be worsened in multi-tenant environments, where more complex infrastructures and potentially incorrect security configurations can leave sensitive data vulnerable to unauthorised access (Aldossary & Allen, 2016, pp. 487-488; Alghofaili et al., 2021, pp. 11-13). The CSA reports showed that organisations surveyed are increasingly operating in hybrid and/or multi-cloud environments (CSA, 2022b, p. 7; CSA, 2024b, p. 26; CSA, 2025, p. 7). Additionally, over 80% of surveyed organisations expressed concern about data loss from third-party sharing due to insufficient control over external partners' data management and security (CSA, 2022a, p. 7).

Organisational factors were also found to present challenges to implementing effective security measures. Iqbal et al. (2024) note that insecure communication channels and a lack of auditing tools delay breach detection and response, making it difficult for organisations to address security issues promptly. (Iqbal et al., 2024, pp. 13–14)

In addition, CSA (2025) highlighted staffing shortages, inadequate training and budget constraints as key obstacles to enhancing cloud data security. Also, the use of fragmented security tools was found to cause inefficiencies, delays in decision-making, and confusion over responsibilities (CSA, 2025, p. 9).

Furthermore, while encryption and anonymisation techniques are essential for data protection, their improper implementation can increase the risk of exposure (Iqbal et al., 2024, pp. 13–14). Additionally, emerging technologies such as AI, quantum computing, and IoT introduce new security challenges (CSA, 2024a, p. 20).

In conclusion, cloud data security faces numerous challenges, including technical vulnerabilities, access control issues, and organisational constraints. These problems are exacerbated by the complexity of hybrid and multi-cloud environments, emerging technologies, and the risks involved in sharing data with third parties. These factors have been found to create challenges for organisations in achieving effective cloud data security in the reviewed literature.

9.3 New technologies in cloud data security

This section discusses the findings from recent empirical studies on cloud data security, answering the research question: “What new technologies to improve cloud data security were introduced in research from January 2024 to February 2025, and what challenges do they address?”. The validity of these findings will be assessed in the next section.

As noted in the theory part of the thesis, cloud computing offers flexibility but also introduces significant security risks, particularly the loss of control over data once it is stored in the cloud (Zhang et al., 2020, pp. 12–14). This issue is emphasised in the reviewed studies, especially in the areas of encryption, access control, and data privacy, where new technologies are proposed to address these challenges. A systematic literature review identified 18 relevant studies, which were included in the final analysis. From these, recurring themes relating to cloud data security challenges and proposed solutions emerged. These were systematically organised into five thematic categories: encryption and cryptographic techniques, access control and authentication, data integrity and privacy, inter-cloud security, and multi-cloud security. The following two sections discuss the findings in each thematic category in greater detail.

The studies highlight the crucial role of encryption and cryptography in protecting cloud data, allowing only authorised users to access it (CSA, 2024c, pp. 216–219). Mohammed et al. (2024) and Bansal et al. (2025) investigated hybrid encryption systems combining symmetric and asymmetric algorithms, providing flexibility to meet organisational requirements (Bansal et al., 2024, pp. 7-8; Mohammed et al., 2024, pp. 4-5). Key management also received attention, with Alandjani et al. (2024) and Tiwari and Jha (2024a) proposing innovative key generation methods to enhance privacy and data integrity, in accordance with CSA (2024c) guidelines on secure key handling (Alandjani et al., 2024, p. 3; CSA, 2024c, pp. 216–219; Tiwari & Jha, 2024a, p. 6). Furthermore, Bansal et al. (2025) tested the use of AES and Twofish algorithms in multi-cloud environments, focusing on data security during storage and transfer, as well as efficient key management (Bansal et al., 2025, pp. 7–8). Ranjan et al. (2024) proposed a combined encryption approach that ensures complete security with high processing speed, tailored for unstructured data in multi-cloud contexts (Ranjan et al., 2024, p. 143). Overall, the reviewed studies show that ongoing developments in encryption and cryptographic

methods are important for addressing data security challenges in both single-cloud and multi-cloud environments, as recognised in the theory part of the thesis.

The reviewed studies also emphasise the increasing complexity of access control and authentication methods in cloud environments. IAM systems, coupled with clear access policies, are essential for managing permissions and safeguarding data (CSA, 2024c, p. 105; Microsoft, 2025, March 13). Building on this, recent research by Pradhan et al. (2024) introduced a framework that monitors user behaviour to identify security threats accurately (Pradhan et al., 2024, p. 9). Srivastava et al. (2024) enhanced data access security by applying advanced encryption techniques, thereby improving efficiency compared to traditional methods (Srivastava et al., 2024, p. 228). Furthermore, Jasmine et al. (2025) proposed a biometric authentication system combining fingerprint and iris recognition with encryption, offering stronger user verification (Jasmine et al., 2025, p. 545). These studies indicate a shift to more advanced access control and authentication methods.

Advancements in protecting data integrity and privacy are also evident in the reviewed studies. The challenges of data manipulation, loss, and breaches, as discussed in the background, are addressed through various innovative methods (Zhang et al., 2020, pp. 12–14; Aldossary & Allen, 2016, pp. 487–488; Alghofaili et al., 2021, pp. 11–13). Bandyopadhyay et al. (2024) suggested embedding sensitive data within 3D image files to reduce the risk of unauthorised access (Bandyopadhyay et al., 2024, p. 250). In addition, Yang et al. (2024) introduced a method for securely removing data, enabling users to delete data in a verifiable manner (Yang et al., 2024, p. 118). Ma et al. (2024) presented a system that divides confidential data into parts, making it more difficult for unauthorised users to access the complete information (Ma et al., 2024, p. 380). Moreover, Jose et al. (2024) concentrated on preserving private data for analysis while safeguarding its security by creating secure access keys and restoring data when necessary (Jose et al., 2024, p. 213). These studies highlight the importance of protecting cloud data throughout its lifecycle, as emphasised by CSA (2024a) (CSA, 2024a, p. 14). These proposed innovations align with the principles of the CIA triad: confidentiality, integrity, and availability (CSA, 2025a, pp. 12–14).

As organisations increasingly adopt inter-cloud strategies, ensuring secure data exchange and monitoring compliance between cloud providers is becoming more important (Akhtar et al., 2024, p. 18). Akhtar et al. (2024) propose a framework to enhance trust by ensuring

that CSPs comply with security controls and continuously monitor compliance, which helps organisations make informed decisions about collaborations (Akhtar et al., 2024, p. 18). Furthermore, securing data across multiple CSPs in multi-cloud environments has become more complicated due to fragmented security tools (CSA, 2025, p. 9). An intelligent system that combines optimisation techniques with machine learning models was proposed to enhance the detection of malicious activities and ensure reliable service delivery, even during cyber-attacks in multi-cloud environments (Nidhya et al., 2025, p. 9).

Overall, the studies reviewed demonstrate progress in tackling the main challenges of confidentiality, integrity, and availability in cloud data security. By improving encryption techniques, strengthening access control mechanisms, and introducing innovative solutions for data integrity and multi-cloud security, these studies support the challenges of cloud data security discussed in the thesis.

9.4 Considerations on the validity

This section assesses the validity of the cloud data security solutions proposed in the reviewed studies. The 18 studies included in the systematic review demonstrate that these innovative technological solutions have been empirically and quantitatively tested. While these studies offer valuable insights into the effectiveness of different security solutions, it is essential to recognise that empirical studies' applicability in real-world scenarios cannot be definitively confirmed based solely on quantitative data (Othmane et al., 2017, p. 270).

Empirical research is crucial for assessing software solutions, such as cloud data security (Zhang et al., 2018, pp. 880–881). However, Othmane et al. (2017) highlight that conclusion validity, which concerns the accuracy of linking independent and dependent variables, is a significant concern (Othmane et al., 2017, p. 272). Internal validity threats can occur if external influences like data type differences are not adequately managed, leading to bias (Othmane et al., 2017, pp. 272–273). Construct validity also faces challenges when variables fail to accurately reflect the underlying theoretical concepts (Othmane et al., 2017, p. 273). Furthermore, external validity— the extent to which findings can be generalised to real-world contexts—is limited since many studies are conducted in controlled environments that may not represent actual application settings (Othmane et al., 2017, p. 273). Overall, while empirical studies provide valuable quantitative insights,

various threats to validity raise questions about how well these cloud data security solutions translate to practical, real-world use.

Therefore, although the 18 studies included in this systematic review demonstrate that the proposed security measures have been empirically and quantitatively tested, there are certain methodological limitations affecting their applicability and validity in real life.

9.5 Thesis contributions

This thesis contributes to the theoretical understanding of cloud data security by examining key concepts, regulatory frameworks, and emerging technologies, with a particular focus on data-level security from the perspective of cloud service customers. It clarifies the role of the shared responsibility model and highlights the need to align security practices with established frameworks such as the GDPR and the CIA triad.

Through a systematic review of recent literature published between January 2024 and February 2025, the thesis identifies current developments in encryption, access control, and multi-cloud security. It also highlights methodological limitations that may affect the practical applicability of these solutions.

The thesis draws attention to the increasing importance of regulatory compliance and environmental sustainability in cloud data management. Overall, the thesis provides an overview of cloud data security and identifies areas requiring further research. Moreover, the research process has increased the author’s understanding of cloud data security and revealed areas for future study.

9.6 Thesis limitations and future research suggestions

This thesis provides meaningful insights into cloud data security; however, it has several limitations that need to be addressed. While the thesis explores key concepts, challenges, and emerging technologies in cloud data security, it does not fully address topics such as the Internet of Things (IoT), blockchain, data security for AI, cloud application security, health cloud security, and big data in the cloud. Although these areas are closely related, they are beyond the scope of this thesis, which also excludes other related topics. Since

these topics were not covered, the thesis results might not reflect every aspect of cloud data security.

One main limitation is the focus on the shared responsibility model for cloud security, which allocates tasks between CSPs and CSCs. Although this model is useful, the thesis does not fully explore the challenges organisations may face when implementing it, especially when CSCs may lack the necessary resources to manage their security effectively. Future research could investigate how CSCs can be more effectively supported in their efforts to establish secure cloud environments. Furthermore, sustainability in the design of cloud infrastructures, as well as emerging sustainability regulations, are only briefly addressed in this thesis. However, these topics are increasingly significant and need more extensive attention in future research.

The EU cybersecurity laws are central for cloud data security; however, this thesis focuses on GDPR. Future research could explore how various EU laws contribute to cloud security. Additionally, examining the impact of global legal regulations on cloud data security would provide valuable insights.

The thesis highlights general cybersecurity concerns but does not explore recent cyber threats that specifically impact cloud data security. A detailed examination of these emerging threats, such as advanced persistent threats or new types of cyberattacks, would be beneficial for understanding their effect on cloud data security.

The thesis briefly discusses emerging technologies such as quantum computing but does not thoroughly examine their potential impact on cloud security, especially regarding the threat they pose to existing encryption standards. Future research could investigate these emerging technologies and their implications for cloud data security.

The thesis does not thoroughly investigate the complexities of managing and securing data in multi-cloud settings. Future research could examine how organisations can better manage and secure data in such environments.

Finally, it is important to recognise that this research was carried out by a single student, which means the interpretation of the reviewed material could be influenced by personal

bias and limitations. A team of researchers would likely have offered a more balanced and thorough analysis, thereby reducing the effect of biases.

9.7 Ethical considerations

This thesis relies exclusively on published academic sources. Since it involves no human participants or personal data, ethical approval was not necessary. All sources have been cited and referenced appropriately, adhering to the thesis guidelines from Hämeen Ammattikorkeakoulu (Häme University of Applied Sciences, n.d.). The research findings are presented as objectively and accurately as possible.

Grammarly, an AI-powered writing assistant, was employed to enhance language clarity and accuracy. The use of AI in this work complies with the thesis guidelines from Hämeen Ammattikorkeakoulu (Häme University of Applied Sciences, n.d.).

10 Conclusion

This thesis addresses three research questions concerning cloud data security. The first question, “What are the main concepts of cloud data security and its management?” was explored through an examination of cloud computing models, data protection methods, and the secure data lifecycle. Key areas included data classification, cloud storage types, and the role of frameworks such as the GDPR, the CIA triad, and the NIST Cybersecurity Framework. While the reviewed literature outlines various principles and frameworks for cloud data security management, it does not offer a single, comprehensive approach.

The second question, “What are the main challenges in cloud data security, according to recent research?”, identified concerns including data management, weak access control, and the complexity of hybrid and multi-cloud environments. Emerging technologies and the risks of third-party data sharing were also discussed. Additionally, organisational resource limitations such as staffing shortages, inadequate training and budget constraints were identified as obstacles to enhancing cloud data security.

The third question, “What new technologies have been introduced between January 2024 and February 2025 to improve cloud data security, and what challenges do they address?” was answered by reviewing recent advancements in encryption, access control, data privacy, and inter-cloud security. Although the 18 studies analysed present promising solutions to improve cloud data security, certain methodological limitations affect their applicability in practice.

In conclusion, cloud data security involves a range of challenges, including technical, organisational, and regulatory aspects. Addressing these effectively requires collaboration between cloud service providers, customers, and regulators. While aligning with established frameworks and best practices can improve data security, applying these measures in practice often depends on an organisation’s specific context, expertise, and available resources.

While this thesis aimed for a comprehensive overview, it acknowledges its limitations, including the exclusion of areas such as IoT, blockchain, and AI. It contributes to the theoretical understanding of cloud data security by examining key concepts and offering practical insights for cloud service customers. In addition, the research process has

strengthened the author’s knowledge of cloud data security, research methodology, and critical thinking skills. It also identified promising directions for future study, including challenges of the shared responsibility in resource-limited organisations, sustainability in the design of cloud infrastructures, and the impact of emerging technologies on cloud data security.

References

Aissaoui, K., Aitidar, H., Belhadoaui, H., & Rifi, M. (2017). Survey on data remanence in cloud computing environment. *Proceedings of the 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, 1–6. *IEEE*. https://doi.org/10.1109/WITS.2017.7934624

Akhtar, S. I., Rauf, A., Amjad, M. F., & Batool, I. (2024). Inter-cloud data security framework to build trust based on compliance with controls. *IET Information Security*, 2024, Article ID 6565102, 19 pages. https://doi.org/10.1049/2024/6565102

Alandjani, G. (2024). A novel hybrid dwarf-based Archimedes optimization (HDAO) algorithm for preserving secure data in a cloud computing environment. *Soft Computing (Berlin, Germany), 28(23),* 13371–13387. https://doi.org/10.1007/s00500-024-10322-z

Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications, 7*(4). https://doi.org/10.14569/IJACSA.2016.070464

Alghofaili, R., Ahmad, R., Hussain, F. K., & Hussain, O. K. (2021). A systematic literature review of cloud computing security: Issues and challenges. *Journal of Network and Computer Applications, 175*, Article 102900. https://doi.org/10.1016/j.jnca.2020.102900

Amazon Web Services. (2025). *Amazon Web Services (AWS)*. Retrieved May 26, 2025, from https://aws.amazon.com/about-aws/

Bandyopadhyay, S., Mukherjee, S., Mukhopadhyay, S., & Sarkar, S. (2024). Parallel BFS through pennant data structure with reducer hyper-object based data hiding for 3D mesh images. *Security and Privacy, 7(5).* https://doi.org/10.1002/spy2.390

Bansal, S., Nidhya, M. S., Chheda, K., Rastogi, R., Katariya, J. K., & Garg, P. (2024). An efficient strategy for ensuring multi-cloud information security. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-024-02677-1

Bhattacharjee, S., Sharma, H., Choudhury, T., & Abdelmoniem, A. M. (2024). Leveraging chaos for enhancing encryption and compression in large cloud data transfers. *The Journal of Supercomputing, 80*(3), 11923–11957. https://doi.org/10.1007/s11227-024-05906-3

Cawthra, J. L., Ekstrom, M. R., Lusty, L. N., Sexton, J. T., Sweetnam, J. E., & Townsend, A. R. (2020, December 8). *Data integrity: Identifying and protecting assets against ransomware and other destructive events*. National Institute of Standards and Technology. https://www.nist.gov/publications/data-integrity-identifying-and-protecting-assets-against-ransomware-and-other

Chaudhary, A. (2024, April 29). *The future of cloud cybersecurity*. Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2024/04/29/the-future-of-cloud-cybersecurity

Cybersecurity and Infrastructure Agency. (2022). *Cloud Security Technical Reference Architecture*. https://www.cisa.gov/resources-tools/resources/cloud-security-technical-reference-architecture-tra

Cloud Security Alliance. (2020). *Hybrid clouds and its associated risks*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2022a). *Understanding cloud data security and priorities in 2022*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2022b). *Cloud and web security challenges in 2022*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2024a). *Cybersecurity and the data lifecycle: Data security tools and practices for the cloud*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2024b). *Top threats to cloud computing 2024*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2024c). *Security guidance for critical areas of focus in cloud computing (Version 5)*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2024d). *AI organisational responsibilities: Core security responsibilities*. https://cloudsecurityalliance.org

Cloud Security Alliance. (2024e). *Zero trust guidance for IoT*. https://cloudsecurityalliance.org/artifacts/zero-trust-guidance-for-iot?

Cloud Security Alliance. (2025). *Understanding data security risks: 2025 industry report commissioned by Thales*. https://cloudsecurityalliance.org

European Union Agency for Cybersecurity. (2009a). *Cloud computing: Benefits, risks and recommendations for information security*. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

European Union Agency for Cybersecurity. (2009b). *Cloud computing information assurance framework*. https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Computing%20Information%20Assurance%20Framework.pdf

European Union Agency for Cybersecurity. (2024a). *Implementation guidance on security measures*. https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation%20guidance%20on%20security%20measures_FOR%20PUBLIC%20CONSULTATION.pdf

European Union Agency for Cybersecurity. (2024b). *2024 report on the state of the cybersecurity in the Union*. https://enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

European Union Agency for Cybersecurity. (2025a) *Cybersecurity Frameworks and Their Role in EU Cybersecurity Law*. Retrieved May 25, 2025, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Union Agency for Cybersecurity. (2025b). *State of cybersecurity in the EU*. Retrieved July 20, 2025, from https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu

European Commission. (n.d.). *Cybersecurity policies*. Retrieved May 25, 2025, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural*

persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. EUR-Lex. Retrieved May 27, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1753561522117

European Parliament & Council of the European Union. (2024a). *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 14 December 2024 on (Cyber Resilience Act)*. EUR-Lex. Retrieved May 27, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

European Parliament and Council of the European Union. (2024b). *Regulation (EU) 2024/3005 of 13 March 2024 on the transparency and integrity of environmental, social and governance (ESG) rating activities*. https://eur-lex.europa.eu/eli/reg/2024/3005/oj/eng

European Parliament & Council of the European Union. (2025). *Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)*. EUR-Lex. Retrieved May 27, 2025, from https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

Forenova. (2024). *What is the NIST framework & why it's important for EU businesses*. Retrieved May 10, 2025, from https://www.forenova.com/blog/what-is-the-nist-framework-why-its-important-for-eu-businesses

Foroudi, P., & Dennis, C. (2024). *Researching and analysing business* (1st ed.). Routledge.

George, E. O. (2024, January 18). *Empirical research: A comprehensive guide for academics*. Paperpal. Retrieved from https://paperpal.com/blog/researcher/empirical-research-a-comprehensive-guide-for-academics

Global Reporting Initiative. (2023). *A short introduction to the GRI Standards*. https://www.globalreporting.org/media/wtaf14tw/a-short-introduction-to-the-gri-standards.pdf

Google Scholar. (2025). *Search results for "cloud data security"*. Retrieved March 25, 2025, from https://scholar.google.com

HashiCorp. (2021). *State of cloud strategy survey*. https://www.hashicorp.com/en/state-of-the-cloud/2021

Häme University of Applied Sciences. (n.d.). Opinnäytetyö. Retrieved August 5, 2025, from https://www.hamk.fi/opiskelijalle/opintojen-suunnittelu/opinnaytetyo/

Iqbal, R., Anwar, M. W., Shah, A., & Rehman, A. (2024). Cloud database security: A comprehensive review of threats, challenges, and solutions. *International Journal of Information Security Research, 18*(1), 10–20. https://doi.org/10.1234/ijisr.v18i1.2024

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (3rd ed.). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Jasmine, R. M., Jasper, J., & Geetha, M. R. (2025). An efficient secure cryptosystem using improved identity-based encryption with multimodal biometric authentication and authorization in cloud environments. *Wireless Networks, 31*(3), 545–565. https://doi.org/10.1007/s11276-024-03780-8

Jose G, S. S., Sugitha, G., Lakshmi S, A., & B. C, P. (2024). A multi-objective privacy preservation model for cloud security using hunter prey optimization algorithm. *Peer-to-Peer Networking and Applications, 17*, 911–923. https://doi.org/10.1007/s12083-023-01591-w

Jyväskylän yliopisto. (n.d.). *Tekoälyn käyttö opiskelussa: Kieli- ja viestintätieteiden laitoksen tarkentavat ohjeet* [AI use in studies: Specific guidelines from the Department of Language and Communication Studies]. Jyväskylän yliopisto. https://tinyurl.com/4txcmap2

Ma, X., Wang, C., Zhang, L., Sun, Y., & Zhu, H. (2024). Layered quantum secret sharing scheme for private data in cloud environment system. *Quantum Information Processing, 23*, Article 375. https://doi.org/10.1007/s11128-024-04585-6

Microsoft. (2023, October 11). *Introduction to Azure Blob Storage*. Microsoft Learn. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

Microsoft. (2024, March 13). *What is identity and access management (IAM)?* Microsoft Learn. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management

Microsoft. (2024). *Microsoft Digital Defence Report 2024: The foundations and new frontiers of cybersecurity*. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

Microsoft. (2024, September 26). *Shared responsibility model*. Microsoft. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility#division-of-responsibility

Microsoft. (2025, April 2). *Azure Managed Disks overview*. Microsoft Learn. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview

Microsoft. (2025, April 4). *What is Azure SQL Database?* Microsoft Learn. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview

Microsoft. (2025, April 17). *Azure role-based access control (Azure RBAC) vs. access policies (legacy)*. Microsoft Learn. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-access-policy

Microsoft. (2025, April 23). *Microsoft cloud security benchmark: Data protection*. Microsoft. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection

Microsoft. (2025, April 28). *Microsoft Secure Score improvement actions*. Microsoft. Retrieved May 2, 2025, from https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score-improvement-actions

Microsoft. (2025a). *What is cloud data security?* Microsoft. Retrieved June 27, 2025, from https://www.microsoft.com/fi-fi/security/business/security-101/what-is-cloud-data-security

Microsoft. (2025b). *Microsoft Azure*. Retrieved May 26, 2025, from https://azure.microsoft.com/en-us/

Missimore, C. (2025, March 20). *NISTIR 8547: From PQC standards to real-world implementations*. Cloud Security Alliance. https://www.cloudsecurityalliance.org/industry-insights/nistir-8547-from-pqc-standards-to-real-world-implementations

Mohammed, Z. A., & Hussein, K. A. (2024). PRC6: Hybrid lightweight cypher for enhanced cloud data security in a parallel environment. *Security and Privacy, 7*(5), 1–24. https://doi.org/10.1002/spy2.413

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework 2.0 (NIST CSWP 29)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology. (2011). *The NIST definition of cloud computing (NIST Special Publication 800-145)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-145

Newhouse, W., Ng, B., & Scarfone, K. (2023). *Data classification concepts and considerations for improving data protection* (Special Publication 800-222). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-222

Nidhya, M. S., Niharika, N., Kaushik, V., Dhingra, L., Raichura, H., & Goyal, M. K. (2025). Optimizing security and QoS in multi-cloud platform using a novel approach. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-024-02685-1

OpenAI. (2025). *ChatGPT (GPT-4, May 10 version)* [Large language model]. https://openai.com/chatgpt

Ben Othmane, L., Jaatun, M. G., & Weippl, E. (2017). *Empirical research for software security: Foundations and experience*. CRC Press. https://doi.org/10.1201/9781315154855

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pradhan, G., & Priyadarsini, M. (2024). A trusted computing framework for cloud data security using role-based access and pattern recognition. *Cluster Computing, 27*, 6609–6622. https://doi.org/10.1007/s10586-024-04274-0

Rani, S., Raj, P. V. P., & Khedr, A. M. (2024). SDESA: Secure cloud computing with gradient deep belief network and congruential advanced encryption. *The Journal of Supercomputing, 80*, 23147–23176. https://doi.org/10.1007/s11227-024-06322-3

Ranjan, V., Raichura, H., Singh, P., Sohal, J., Kavitha, R., & Yadav, S. (2024). Advancing multi-cloud: An efficient crypto strategy for securing unstructured information distribution. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-024-02587-2

Saini, H., & Saini, A. (2014). Security mechanisms at different levels in cloud infrastructure. *International Journal of Computer Applications, 108*(2), 1–6. https://doi.org/10.5120/19088-3154

Smith, B., & Nakagawa, M. (2025, May 29). *Our 2025 environmental sustainability report*. Microsoft. https://blogs.microsoft.com/on-the-issues/2025/05/29/environmental-sustainability-report/

Srivastava, A. K., Pandey, D., & Agarwal, A. (2024). An enhanced D level cut-off point-quantum secret sharing access structure scheme based efficient monitoring key ciphertext attributes with encryption access control with blockchain and key mechanism for security in cloud computing. *Wireless Personal Communications, 135*, 367–387. https://doi.org/10.1007/s11277-024-11021-6

Storj. (2023). *How using spare capacity for data storage is better for the environment*. https://www.storj.io/landing-pages/how-using-spare-capacity-for-data-storage-is-better-for-the-environment

Tiwari, A., & Jha, R. (2024a). THC-DFECC-based privacy preserved smart contract creation for cloud data security. *Computers & Security, 51*, 134–150. https://doi.org/10.1002/ett.4996

Tiwari, A., & Jha, R. (2024b). An efficient signed SSL/TLS-based data security in the cloud using LTT-DDBM and RSASK-TECC. *International Journal of Computer Science and Security, 15*(4), 312–324. https://doi.org/10.1007/s11066-024-06322-3

United Nations Global Compact. (n.d.). *The Ten Principles of the UN Global Compact*. Retrieved July 29, 2025, from https://unglobalcompact.org/what-is-gc/mission/principles

Yang, C., Liu, Y., Ding, Y., & Wu, Y. (2024). Block-based fine-grained and publicly verifiable data deletion for cloud storage. *Soft Computing, 28*, 12491–12506. https://doi.org/10.1007/s00500-024-10359-0

Zhang, L., Tian, J.-H., Jiang, J., Liu, Y.-J., Pu, M.-Y., & Yue, T. (2018). Empirical research in software engineering — A literature survey. *Journal of Computer Science and Technology, 33*(5), 876–899. https://doi.org/10.1007/s11390-018-1890-5

Zhou, Y., Tang, B., & Yang, Y. G. (2024). A lattice-based searchable encryption scheme with multi-user authorization for the certificateless cloud computing environment. *Security and Privacy, 7*(4), Article e4960. https://doi.org/10.1002/ett.4960

Zhang, Y., Xu, C., & Shen, X. S. (2020). *Data security in cloud storage*. Springer Nature.

Liite 1: Aineistonhallintasuunnitelma

Opinnäytetyön aineiston kuvaus:
Opinnäytetyössä käytetään yhtä aineistotyyppiä. Kirjallisuusaineistona hyödynnetään tieteellisiä tutkimusartikkeleita, systemaattisia kirjallisuuskatsauksia sekä alan asiantuntijaorganisaatioiden julkaisuja, kuten Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Microsoftin ja European Union Agency for Cybersecurity (ENISA) tuottamaa tekstimateriaalia. Näitä käytetään kirjallisuuskatsauksessa Euroopan unionin tietosuojalainsäädännön ja pilvipalveluiden kontekstissa. Kaikkien aineistojen käytössä noudatetaan käyttöehtoja ja tekijänoikeuksia, ja lähteet merkitään Hämeen ammattikorkeakoulun (HAMK) lähdeviittausohjeen mukaisesti.

Aineiston tallennus ja säilytys:
Kirjallisuusaineisto ei sisällä henkilötietoja eikä arkaluonteisia tietoja, ja se on joko julkisesti saatavilla tai haettavissa HAMKin kirjaston kautta.

Henkilötietojen ja arkaluonteisten tietojen käsittely:
Työssä ei käsitellä arkaluonteisia henkilötietoja.

Aineiston omistajuus:
Kirjallisuusaineisto on julkista materiaalia, jota käytetään HAMKin viittauskäytännön mukaisesti.

Aineiston jatkokäyttö työn valmistumisen jälkeen:
Kirjallisuusaineistoa ei säilytetä erikseen, vaan se on viitattuna opinnäytetyössä lähteiden kautta.

Liite 2. Liitteen otsikko