International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Cloud Security Best Practices: Strategic Measures to Protect Digital Assets Within the Cloud

**Richard Aggrey[1], Afeti Cudjoe[2], Karl Osei Afoduo[3], Bright Ansah Adjei[4], Nana Adwoa Konadu Dsane[5], Jessica Eyeson[6]**

[1]Dep. Director, Head of IT, University of Ghana Medical Centre
[2]IT Consultant, University of Ghana Medical Centre
[3,4]Senior Health Research Officer, University of Ghana Medical Centre
[5]Dep. Director of Research, University of Ghana Medical Centre
[6]Research Assistant, University of Ghana Medical Centre

**Abstract**

This paper intends to explore the key features of cloud security, highlighting core practices and strategies in data and application protection within cloud setups. First, it explains cloud computing and the different types of services - service models and deployment models. It subsequently centres on cloud security, detailing the potential risks and threats that could occur, including data breaches and account hijacking. The paper also covers fundamental security practices to reduce these risks, such as data encryption and access control. Thus, to establish the security of information saved on a network during the process of transmission, data encryption must be carried out. In the same vein, user management methods such as Role-Based Access Control (RBAC) and multifactor authentication must be enabled and enforced to minimise access to sensitive information and systems. The need to protect cloud applications is also addressed, emphasising the importance of application security testing and container security. Therefore, each stage of the application development lifecycle can be secured, reducing vulnerabilities and the potential for attacks. Finally, the paper includes a discussion on cloud security compliance and regulation. Organisations must adhere to specific standards and regulations to secure sensitive data and meet the various requirements. By fulfilling these requirements, organisations can avoid legal and reputational risks.

## 1. Introduction to Cloud Security

It is widely known that businesses rely heavily on cloud services, as securing data and applications in the cloud is crucial. Today, cloud services are fundamental to companies' operations, transforming the way they support, secure, and engage with their services (Srinivasan et al., 2021). As a result, cloud security and compliance have become utmost priorities at the executive level, across industries, and within any organisation serving a global community. The increasing reliance on cloud technology and expanded storage capacity has prompted many businesses and industries to shift their assets and information to cloud computing services (Sharma & Gupta, 2022), moving away from localised or on-premises solutions.

Securing data and applications in the cloud requires new strategies that differ from traditional security pra-

tices. While the fundamentals of unauthorised access, maintaining data and system integrity remain universal; the scope of responsibilities has expanded. Cloud security now requires attention to risks beyond data leakage and physical security of datacentres (Parast et al., 2022). The shared responsibility model means that adequate cloud security is a joint effort between the customer and the cloud service provider. In addition to shared responsibility, cloud security presents unique challenges due to the transient and dynamic nature of cloud environments. Security is no longer simply about aligning network security policies with network elements; instead, it requires corresponding policies for instances or systems. As new instances are recreated or updated, policies must evolve to reflect these changes. Furthermore, as instances failover, scalability rules are utilised, or other configurations are changed, network access and security policies must adapt to these dynamics to accommodate high availability and failover without increasing attack vectors. The evolution of cloud computing has had a significant impact on security and networking. There are distinct threats and risks when managing private, public, or hybrid cloud environments (Tabrizchi et al., 2020).

### 1.1. Overview of Cloud Computing

In recent years, the use of cloud computing has increased remarkably. Cloud services are typically self-service and available on demand. Cloud service users do not control, or need to maintain, the underlying computing infrastructure. However, they retain control over deployed applications and, to some extent, the configurations of the application hosting environment. Cloud computing provides a facility for outsourcing computational and storage requirements to third-party data centres. From processing power to data storage to infrastructure security, it offers all these computing resources (Goswami et al., 2024).

Key attributes of cloud computing solutions essentially in line with the NIST framework include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services, distinguishing it from traditional computing. Cloud computing, mostly referred to as the natural evolution of the internet and ubiquitously as "the cloud". It is a connective architecture that enables the storage and processing of large amounts of data. Users can benefit from various service models offered by cloud computing (Gao et al., 2020). The cloud infrastructure supports three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS).

In IaaS model, clients purchase storage, processing, networks and infrastructure components hosted in the cloud. The PaaS model helps to execute various programming languages and other software programs that support web services. With the PaaS, clients can rely on more scalable infrastructure as the cloud provides the required software components. The SaaS model permits users to use software applications derived from the internet. The deployment model creates the advantages of cloud computing regarding scalability and savings on IT costs. Depending on the requirements and where the workloads are deployed, cloud deployment models are divided into four according to the needs of the workloads (Maaz et al., 2023). They are:

- Public Cloud
- Private Cloud
- Hybrid model
- Community model.

### 1.2. Importance of Cloud Security

Technological advancements have significantly impacted operational paradigms, with most businesses sharing one common feature; reliance on cloud-delivered services to some extent. The growing adoption of cloud computing for everyday business operations, which rely on constant access to services and storage

resources, has driven increased consumption of cloud technology. However, the rising adoption of cloud technology also exposes organisations to the inherent intricacies of such complex ecosystems. Data breaches' potential to impact service providers and users is a significant concern. As the cybersecurity threats landscape grows more sophisticated, so do the risks to personal privacy and the loss of sensitive personal or business data. For this reason, cloud security practices have become a necessity to assuage customers' fears regarding the potential sharing of private and personal information with third parties. These concerns are heightened by organisations' legal obligations to know where their cloud provider stores customer and client data. Regulatory compliance and the establishment of robust data security protocols are essential components of cloud security (Oladoyinbo et al., 2023).

Unauthorised access, data breaches, and data leakage are particularly challenging in cloud environments, compounded by the scale and potential impact of such violations. However, these are not the only challenges associated with integrating cloud services into business operations. Web-based services, especially in the cloud, must prioritise the surveillance of cyber intruders and implement reversible encryption to protect data, as it is impossible to fully secure data in cyberspace. Violations, whether caused by digital infections or other threats, generate significant concerns about damage to public perception and financial losses. Having the power not only to intimidate or hurt customers, but also the loss of revenue streams and reputation, organisations have an obligation to stay on their toes and be proactive (Ahmad, 2022).

This is a dynamic space, and as the technology creates more opportunities for breaches, the risk management strategies we create need to continue to change and evolve by finding continuous monitoring features. A risk-based approach to cloud security is the only solution to the challenges faced by decision makers across the private and public sectors domestically and globally. If you don't understand this, your efforts at ranking and prioritising risks won't produce much value. When information security is properly implemented, it should transcend the debate between "cyber" versus "non-cyber" or "IT support" versus "value-added service." In fact, a well-executed information security strategy makes this debate irrelevant, as value-added services become an integral part of overall business strategy, rather than simply serving as IT support or cost centres (Thabit, 2020).

## 2. Key Threats and Risks in Cloud Environments

Cloud environments offer many benefits to organisations including cost efficiency, flexibility, scalability, capacity, and business continuity (Ahmed et al., 2023). However, when compared to on-premises environments, cloud environments present several serious and occasionally complex threats to data and applications. Employees, often referred to as superusers have their hands on everything – machine data filtering in storage and computing, metadata, or sensitive raw data records at the server end. External threats include brute force attacks and advanced hacking, cross-site scripting, Denial of service (DoS) and Distributed denial of service (DDoS). Additionally, insider threats are considered to be more dangerous in many organisations (Arif et al., 2024).

The virtual environment amplifies these challenges. Perpetrators typically use software designed for port scanning in virtual environments to gain access to sensitive data. Once access is achieved, attackers use various proprietary and open-source utilities to recover phantom data blueprints. Studies indicate that around 60% of attacks on cloud environments are linked to espionage or data theft (Cybersecurity Ventures, 2022). Reports have identified cloud vulnerabilities such as account hijacking as a major threat, with endpoints in the cloud's web application interface listed as the fifth most significant security threat

(Smith et al., 2023). The interception of sensitive data remains the top threat on this list. Account hijacking, which was initially ranked as the nineth most significant threat, has now risen to the fifth place, accounting 48.5%. This represents a 10% year-on-year increase in account hijacking threats (Jimmy, 2024).

### 2.1. Data Breaches

Given the advances in cloud computing, it is troubling that the risks of data and application breaches in the cloud have led to an increasing focus on securing data and application in the cloud. Generally, a data breach refers to the unauthorised access to or disclosure of numbers and information generated, stored and processed within information systems, or their modification, loss or deliberate destruction. Hacks and malicious organisations are among the main causes of most data breach. For any affected organisation, a data breach can lead to legal actions from regulatory authorities, stiff fines, mandatory corrective actions, damage to an organisation's reputation, loss of customer trust, and missed longer-term business opportunities. Oftentimes, another consequence of a data breach is fraud and identity theft (Vallabhaneni, 2024).

While various types of data breaches can occur across different domains, two major categories are particularly relevant in cloud environments:

- **Unauthorised access breaches:** These involve attempts to gain unauthorised access to a service. This could include accessing a machine hypervisor or another service running within the same or a different guest/tenant operating system within a cloud deployment. When such unauthorised attempts involve intelligence gathering to identify vulnerabilities that could reveal user data, they highlight the financial value of data and the threat these breaches pose to organisations. Unauthorised access to web services is especially noteworthy, since these services are often public rather than confined to virtual machine creation. Once detected, unauthorised access event is promptly added to investigation lists (Aslan, et al., 2023).
- **Unauthorised access vulnerabilities:** These allow hackers to gain access to sensitive information such as emails, usernames, passwords, and transaction records. This can result in various attacks, including backdoor access, file infector malware, and XML query language (XQL) attacks. The exploited vulnerabilities are typically associated with overwritten software servers, and reverse-engineering and this exploit is often an effective response.

Data leakage caused by hardware vulnerabilities also poses a significant threat to cloud infrastructure. Within hours of a major vulnerability announcement, attackers reverse-engineered the exploit, created a working variant, and infected live targets. In some cases, scripts have been exfiltrated from active Blockchain nodes, leading to malicious transactions (Bhadouria, 2022).

### 2.2. Account Hijacking

It is important to note that account hijacking is a constant threat to cloud environments. Some of the tactics that are often employed by the attackers include using of malware, phishing or credential stuffing among others. Likewise, Account Hijacking refers to the unauthorised use of third-party applications or services to compromise cloud accounts and thus put the digital assets at risk and affect business processes. These attacks mainly aim at the weaknesses of the authentication mechanisms of the cloud services. The most common target of the attackers are insider and user accounts especially in large organisations. According to Mostafa et al. (2023), more than 20% of account-related attacks lead to loss of over $2. 5 million.

**Mitigating the Risk:** Multi-factor authentication (MFA) is quite effective in improving identity verification and reducing chances of an account hijacking. An attacker would only be successful if the several layers of MFA are cracked, far less likely compared to static passwords, which are mostly the

targets of bad actors. The strength of MFA rises with the diversity and quantity of authentication techniques used, forming a strong barrier against attempts to hijack accounts (Said et al., 2022).

## 3. Case Studies of Data Breaches

### 3.1.a. Toyota Motor Corporation: May, 2023

Toyota Motor Corporation reported a data breach that compromised approximately 260,000 customer records. The breach was attributed to an unsecured cloud environment resulting from inadequate dissemination and enforcement of data handling rules.
To address the predicament, the organization established a system to consistently oversee and validate th e configurations of its cloud environments, performing daily assessments to guarantee compliance and se curity (Toyota Motor Corporation, 2023).

### 3.1.b. Tesla Inc: May 2023

Tesla suffered a data breach that revealed the personal information of around 75,000 individuals, including names, addresses, phone numbers, employment information, and Social Security numbers. Two former employees of the organisation were attributed to the breach, who shared the information with a German newspaper. Although the newspaper declined to publish the information, Tesla responded by filing lawsuits against the former employees and confiscating their devices (Croft, 2023).

### 3.1.c. Uber Technologies Inc: September, 2022

In September 2022, Uber suffered a data breach that exposed 57 million sensitive records belonging to customers and employees. The attackers orchestrated a social engineering campaign to infiltrate the organisation's internal systems. They exploited a PowerShell script containing domain admin credentials, which provided access to Uber's cloud platforms and internal employee dashboards. To address the breach, Uber collaborated with law enforcement and kept the public informed by posting updates on their website (Shachnow, 2022).

## 4. Best Practices for Securing Cloud Data

Many organisations fall into the trap of being reactive choosing not to invest in security until problem arises (Miller & Jones, 2020). This approach contrasts sharply with the proactive attitude required for cloud security, particularly when it comes to safeguarding your data. Early prevention, can save significant headaches and costs in the future. Basic but essential practices include encrypting data, code, and applications (Gupta et al., 2020). Encryption guarantees that information is protected at rest or in transit by keeping it unreachable without the appropriate decryption tools. Although encryption cannot stop data theft, it makes the stolen data ineffective for malicious individuals (Zhang et al., 2020).
Moreover, if attackers cannot read the data, they cannot exploit or sell it. Access controls are another cornerstone of effective cloud security. The primary goal is to ensure that systems and applications are protected in such a way that only authorised users are able to access them. There are several techniques which are used in order to achieve this goal and some of them are Principle of Least Privilege (PoLP) and Role-Based Access Control (RBAC). The resultant effect, minimises data exposure by assigning relevant permissions to users to keep them from having unrestricted access. In furtherance to that, the aforementioned techniques can simplify and automate other security policies enhancing the overall security posture and ensuring compliance with regulatory requirements.
As a mandatory requirement, conducting regular audits, ideally on annual basis, allows administrators to gain a comprehensive view of user access and privileges. Furthermore, understanding data access insights

is essential for recognising abnormal behaviour and implementing immediate corrective measures. What's more, deploying DLP solutions enhances security by averting data breaches, thereby preventing unauthorised data transfers from leaving the network. This solution can track the ingress and egress of the network as well as implement policies to protect sensitive information. For instance, DLP can protect data like credit card numbers, Social Security numbers, and other valuable documents from being sent through email, chat, or other cloud applications. By deploying a DLP system, organisations can significantly reduce the risk of data loss (Gupta et. al., 2020).

### 4.1. Data Encryption

Data encryption is a data security measure for information stored at rest and in transit, designed to prevent unauthorised access by malicious actors. Data is transmitted at transient speeds through secured networks, but it is commonly encrypted as a best practice. Encryption is a complex field and the focus of ongoing research, because even the best encryption technology available today may become outdated with the development of sufficiently advanced hardware. Emerging research areas include post-quantum encryption, secure multiparty encryption, Public Key Infrastructure (PKI), and Blockchain encryption technologies, as well as methods for mitigating password encryption vulnerabilities. Since symmetric and asymmetric encryption is computationally intensive in cloud computing, the time required for encryption and decryption is a critical factor in the environment (David et al., 2022).

Various technologies support encrypting data at rest in environments, such as Trusted Platform Modules, file and folder encryption, and database encryption. The primary standard for at-rest encryption in the cloud is Advanced Encryption Standard (AES). Other standards, like Serpent or Two fish, are less common. There are several considerations for securely providing encryption keys to the server, such as grounded key management or Hardware Security Modules (HSM). Ultimately, the greatest vulnerability in encryption security lies in abysmal key management, as access to encryption keys can decrypt the data regardless of the encryption's size or complexity. Encryption establishes a known security boundary for organisations and is recommended as one part of a comprehensive and ongoing cloud data security improvement strategy (Shakor et al., 2024).

### 4.2. Access Control

Access control is the cornerstone of security in the cloud. A robust access control policy is quintessential to ensure that users cannot access any data or application they are not authorised to view. At its most basic level, this involves creating policies that define who have access to what and the associated access levels. Securing access in hybrid or multi-cloud environments is more complex because it requires managing a combination of applications, cloud providers, and private data centres. Once these details are resolved, the next step is to determine the credentials users need to authenticate themselves to access the data or applications. Policies are usually tied to groups of users with similar data permissions or job roles (Kayes et al., 2020).

Identity and access management solutions can simplify the challenges of user administration, password management, and access policy enforcement. Identity management solutions manage the entire lifecycle of a user at a central point and are often integrated with Single Sign-On (SSO). Authorisation governs access to data and applications using solutions such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). Access is granted based on the principle of least privilege (PoLP) – users can only access the data and applications required for their jobs. For groups that do not need access to certain data or applications, relying on authentication without further validation could result in a security breach. One common method to mitigate such risks is multilevel authentication or Multifactor

authentication (MFA). By requiring users to provide two or more independent credentials, MFA reduces the risk of a security breach if one credential is lost or stolen. Access controls are consistent, ensuring that users who gain access through a cloud-based portal retain appropriate access when transitioning to on-premises systems or other cloud services (Patil et al., 2023).

It is important to regularly review and test access control policies to understand risks and to update the rules and policies as needed. This process may include adjusting configuration settings, preferential access and access controls, rule-based alerts on all devices, applications, and the data centre. Access control is, therefore, one of the most critical security practices for protecting data, applications, and workloads in the cloud from misuse, compromise, or loss of integrity (Jangjo et al., 2022).

### 4.3. Zero-Trust in Cloud

Today, with the increasingly sophisticated attacks that are prevalent, organisation need to adopt a "Zero-Trust" approach. Rather than trusting everything solely because it originates from within the network, no user or system, whether inside or outside the organisation, should be trusted by default and access must be continuously verified. The traditional security paradigms of "trust but verify" and "protect the perimeter" are now outdated. This new approach ensures constant verification. In a modern organisation with remote workers, disparate systems, and distributed data, perimeter-based protection is no longer sufficient. Instead, every interaction within and around the network requires verification. Security today should be a state where no implicit trust is granted to any system solely by virtue of its location or environment, whether attached or detached (Chinamanagonda, 2022).

A Zero-Trust approach takes risk into account and enables continued business operations through effective security management. Beyond security monitoring and operations controls, Zero-Trust serves as an organisation's strategy for delivering secure and reliable services in legacy, cloud, and hybrid enterprise environments. The cloud presents numerous challenges for providing a Zero-Trust environment. Building cyber defences within the cloud requires the enforcement of security and governance policies. This enforcement might include custom firewall rules, anti-malware gateways, and endpoint protection service configurations. Currently no unified standards exist for the security and compliance precautions that must be enforced; instead, there are only fragmented, industry-specific regulations. Because of the unique power and flexibility of the cloud, completely new tactics and strategies must be devised to operate a cyber-secure posture (Mehraj et al., 2020).

#### 4.3.1 Key Principles of Zero-Trust Architecture

Implementers and proponents of Zero-Trust Architecture rely on four principles to guide its planning and implementation. While some may word these principles differently or combine them, these basic tenets should form the foundation of any Zero-Trust project. These principles are: Verify Every User, Validate Every Device, Least Privilege, and Assume Breach. These tenets can interact and reinforce each other, but they constitute the core framework on which Zero-Trust has been built and understood for the past twenty years. For instance, the principle of least privilege is central to Zero-Trust typically defined as granting only the necessary authorisation for a system user to complete a job or function (Stafford, 2020).

Zero-Trust presumes that every internal and external network could possess threat. Even after verifying the identities of devices and users, it further segments networks into tiny areas. This practice, known as micro-segmentation, was held back in the past because it required the management of vast quantities of subnets. With Zero-Trust Architecture, networks are segregated into thousands (or millions) of virtual network segments, because every Zero Trust strategy must secure each micro-segment thoroughly,

solutions like artificial intelligence and machine learning may assist in identifying retail point-of-sale systems versus malware. It also means the core of Zero-Trust Architecture denies the trust authorised by both the organisation and its employees in favour of suspicion (Collier et al., 2021).

Additionally, robust identity and policy management systems are employed. Strong authentication protocols are deployed, and data is encrypted at rest, in transit and in use. Once the correct user and device are confirmed, organisations must log and monitor user behaviour as well as the integrity of the environment its assets. Regular reviews and refinements of policies and technology controls are essential to maintain compliance with laws and regulations (Apeh et al., 2023).

## 5. Securing Cloud Applications

The scope of cloud security naturally includes the protection of applications hosted within cloud environments. Regardless of where an application is hosted, security should be integrated throughout the software development lifecycle and the operations phases (Pearce et al., 2022). Application security is not just an internal IT focus, but rather a shared responsibility of all stakeholders. It is the first line of defence and the central protection pillar for customers, partners, and the business. By adopting proactive security best practices, organisations can address issues, react to new threats, and stay ahead of the attackers (Ahmad et al., 2021).

A critical step for organisations is conducting security testing on cloud-deployed applications prior to launch. This proactive approach to help uncovers and remediate security vulnerabilities. When implemented and monitored, the following components provide a comprehensive perspective on cloud application security:

- Top web application security vulnerabilities
- Application security verification standard
- Top application security risks

Most vendors and open-source tools support both static and dynamic analysis. The primary advantage of static code analysis over other methodologies is that it is performed during the development phase, before the programmes are actually executed. Container security has become a critical perimeter in cloud-based application security due to the increasing adoption of containers (Casalicchio & Iannucci, 2020). Another significant concern is securing APIs, which are the most common entry point for attackers to target or exploit vulnerabilities. To facilitate the automation and integration of application security into cloud environments, architectural guidance and recommendations are provided for building and integrating secure application development toolchains (Rangnau et al., 2020).

### 5.1. Application Security Testing

Application Security Testing (AST) is defined as the process of enhancing the development environment with the aim of minimising security vulnerabilities; It is a process of assessing the vulnerabilities of an application and risks that can be identified during the software development process. Most application security vulnerabilities can be significantly reduced if they are identified by source code tools and then manually verified before production. This process is also considered in the non-development stages of the Software Development Lifecycle (SDL). AST is implemented to fortify the security of applications, primarily by identifying security bugs to enhance the application's security posture (Ratta et al., 2021).

In the present security scenario, the need of the hour is to implement a proactive stance on application security to deliver secure products to customers. Cyber threats are evolving rapidly, shifting focus on the

application layer. As such, conducting security checks is crucial, as application security testing suggests. Security testing has been integral to various initiatives and methodologies over the years. While in the past, it was conducted at the end of the development process, organisations are now integrating security into agile development methodologies and DevOps practices. In the current era, many advisory bodies and standards recommend a proactive rather than reactive approach of security. This approach suggests that security should be integrated into the lifecycle. This proactive stance involves in-depth defence measures for application security, where the superficial checks made at the end of the Software Development Lifecycle SDL are supplemented with deep and practical checks made at the engineering and business levels (Pearce et al., 2022).

### 5.1.1 Methodologies for Application Security Testing

The integration of automated and manual testing strategies is the most effective approach for evaluating cloud enabled applications. So Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (SAST), and Software Composition Analysis (SCA) each have distinct advantages and disadvantages. Selecting the best tools based on these characteristics requires organisations to understand these methodologies and identify the most appropriate combination for their business context. Organisations need to understand the environment in which the application will be tested, including supported languages, security mechanisms, engines and other provider or premises-based security testing considerations (Biswas et al., 2023).

### 5.1.2 Benefits of Security Testing

Security testing is an engaging but indispensable phase of software development that safeguards against data leakage and fraud. It helps to retain user trust and protect the organisation’s reputation. Organisations that integrate a security monitoring system into their software development will ensure continuous actionable vulnerability testing. This approach results in reduced false positives and greater integration into the development infrastructure.

In the event that the system informer, for instance, finds several vulnerabilities, such as default credentials and hard-coded private keys, backdoor administrative port applications, and privilege escalation backdoors, the best approach would be for the enterprise to remediate these threats. Addressing vulnerabilities promptly prevents them from escalating to partners or vendors, thereby improving the overall security posture. Moreover, software security issues are exposed that administrators were unaware of because of an established trust for software developers being secure (Golightly et al., 2022).

### 5.1.3 Avoiding Pitfalls in Application Security

Application Security Testing varies continually; as such, the testing strategy must be flexible and adaptive to address different uses, threats, and vulnerability vectors. Conventional web application security testing primarily consists of penetration testing conducted on the final product before delivery to the customer or launch. While penetration testing is crucial, application security should be a continuous effort that leverages every available avenue to mitigate risks and weaknesses throughout the development lifecycle, from the initial concept to the final deployment (Chirra, 2020).

In today’s dynamic development culture, telling employees they “should" do something without providing data or actionable steps to help them achieve a goal is insufficient for driving security changes. Engineering and cloud companies should foster a culture that integrates security into the development process. Accurate, industry-grade testing with realistic standards and transparent reporting can generate usable, actionable datasets. Furthermore, expanding exploration into containers and functions as a service

for organisation-wide security will enable engineers and developers to better evaluate risks and architectural design trade-offs (Segun-Falade et al., 2024).

### 5.2. Container Security

Containers are packages that host an application, its libraries, runtimes, and other components. In addition to the application code, they include the environment and metadata needed to run the application. Containers abstract away the operating system and hardware dependencies, allowing applications to run on any system, regardless of configuration. They have become increasingly popular in cloud deployments because of their portability and require less overhead than traditional hypervisor-based virtual machines. However, containers pose a new set of security challenges. All necessary components exist within the container, from the operating system to the application dependencies, making everything critical to the security of the containerised application. If a container is compromised, the attacker gains access to the entire application environment, thus it is essential to secure containers at every step of their lifecycle, from building to production (Casalicchio et al., 2020).

What's more, due to their advantages, containerised applications continue to be widely adopted. Container security best practices start by confirming the integrity of a container and its contents, ensuring that they are protected and hardened. Additionally, regular security monitoring is necessary to ensure the container environment remains secure over time. Effective container security strategies require an incident response plan tailored to these environments. Containers operate at a higher level than the virtualisation layer, so the security, compliance, and segmentation requirements differ. Finally, all security practices should align with industry standards wherever applicable (Rice, 2020).

### 5.3 Cloud-Native Security

Cloud computing solutions have transformed the enterprise sector by revolutionising the way businesses operate. Cloud-native techniques and processes have become the new standard. Cloud computing solutions have transformed the enterprise sector by revolutionising the way businesses operate. Cloud-native techniques and processes have become the new standard. This solution utilises cloud services for scalable application development in modular and distributed environments, marking a shift away from traditional on-premise, firewall-based security paradigms (Deng et al., 2024).

Securing these new environments requires a fresh approach due to the changes in architecture and operations. This transformation has introduced a new set of challenges – the security of the cloud. With security methods and tools adapted to meet these changes, security becomes an essential ingredient instead of a bolted-on consideration in cloud-native environments. Organisations must develop a security-first mindset and integrate best practices directly into development and operations pipelines. Legacy security methods fail to ensure data integrity and privacy in cloud environments, as attackers adopt innovative techniques exploiting constant new threats and vulnerabilities with advanced tools and methods. (Mustyala, 2023).

#### 5.3.1 Key Concepts and Principles of Cloud-Native Security

Integrating security concepts into cloud-native technologies like microservices, containers and Kubernetes is critical. Chief among these concepts is Security by Design, which involves integrating security into every stage of the System Development Lifecycle. Organisations appreciate the need to embed security within a comprehensive risk management strategy. With the ongoing digital transformation of organisations, security must now be fully integrated into agile methods of project development. The Zero-

Trust model assumes that even though an entity has gained access to some part of the network, it should not automatically have implicit access to other parts without explicit verification (Butpheng et al., 2020). Another point to consider is that access can change, thus, it is a dynamic and ongoing process that should be continuously verified as in the Zero Trust principle. Regulatory requirements can dictate security strategies in using cloud-native technologies to ensure that data is secure, such as mandating the use of encryption mechanisms. Secure cloud-native software should proactively identify potential threats, with a focus on flexible and adaptive security plans. Threat modelling exercises can be conducted using a range of methodologies, from comprehensive frameworks and guidelines to simple, easy-to-use tools in tandem with this, vulnerability management is the cyclical practice of identifying, classifying, prioritising, and mitigating software weaknesses. It can be performed regularly or when expected software and hardware changes occur (Patel, 2024).

**6. Compliance and Regulatory Considerations in Cloud Security**

Compliance and regulations are serious concerns when adopting cloud security initiatives. Numerous regulations apply to organisations and industries; with guidelines established by industry groups, governmental, and non-governmental bodies (Li et al., 2021). Failing to adhere to these governance requirements incurs tough penalties and damage to the organisations' reputation. Security controls must be kept in place by organisations in order to protect data against external threats and to live up to industry regulations (Li et al., 2021).

Many regulatory standards were established long before the modern technology shift began. However, today's security activity and spending primarily focus on data, applications, and services as organisations migrate to cloud-based systems. Any new work still housed in on-premises systems is subject to less scrutiny and attention, largely due to the complex and costly licensing in many traditional backup and security tools. Still, regulation and compliance requirements have not decreased (Pero & Ekman, 2023). Regulations and standards continue to be written and enforced for data residing on-premises because organisations have not fully migrated to cloud data storage. It is very hard for an organisation to achieve these goals successfully without extensive documentation and thorough audits. Leadership needs trusted sources for promotion, and all internal employees want reliable sources to trust their data security and that of their organisation. This is a significant public accountability issue. If we accept the push to leverage the cloud more effectively, we must address the compliance and security requirements (Pero et al., 2023).

To protect themselves and their citizens, U.S. government enacted personal information breach notification and data embargo laws. If an organisation violates its data use and disclosure policies, it may be responsible for lawsuits on multiple fronts, including class action lawsuits from affected individuals. There may also be penalties from regulatory bodies. These can be avoided by ensuring and verifying that robust security protocols are in place to secure an organisation's cloud system properly. To earn the public and the stock market's confidence, senior management must invest in the security of their organisations before something goes wrong (Li et al., 2021).

The impacts of regulatory and compliance mandates signal the importance of maintaining security operations, ensuring data safety, communication with auditors, and implementing overall security work processes for stakeholders. Keeping up with the changing landscape of legal and regulatory mandates can be a full-time job, requiring frequent training classes and plain old-fashioned reading. Consequently, highly skilled administrators can also be employed to monitor systems for security breaches. While security operations personnel can assure system integrity, if human mistakes are not eliminated, they will

soon detect moments of human error in an unpredictable manner. For instance, when an employee noticed a change in organisational data, one of the largest recent cloud system hacks was identified. Once a breach has been detected, organisations need to work with security specialists to eliminate routine activities that take place. Compliance this month does not mean the organisation can forgo it for the next few months. Staff must be sufficiently trained and focused to build this kind of environment (Alghofaili et al., 2021).

## 7. Ethical Implications of Cloud Security

### 7.1.a. Privacy Concerns in Cloud Computing

Cloud computing can be defined as a model for delivering virtual computing utility which involves the use of the internet to access a variable set of computing resources. It enables the user to back up and process data in large quantities using remote servers without incurring the costs of setting up the necessary infrastructure. The top cloud providers guarantee that state-of-the-art security measures have been put in place to prevent misuse of data, unauthorised access, damage or any other form of violation (Alouffi et al., 2021). However, a series of issues can raise eyebrows from an ethical and privacy standpoint.

Due to the nature of cloud computing, security and privacy threats are closely linked with one another (He & He, 2020). Sensitive personal information is often stored on remote servers or transmitted between personal computers and the cloud server. Data breaches can result in financial and reputational losses for the provider, as well as expose the persons involved in identity theft and other security issues. Furthermore, the use of cloud services is predicated on subscribers' ability to keep, exchange, and disseminate their data with other users and/or services; hence, the use of cloud technology exacerbates difficulties related to data privacy and sharing. The improper disclosure of data by authorised parties has affected a significant percentage of organisations participating in surveys. Increased data exposure intensifies the need for user consent over data management and transparency over the practices used by service providers to protect such privacy. In addition, an individual's data can be persistently stored across multiple servers. While some data centres have policies around data destruction, reports indicate that a considerable percentage of small and medium-sized businesses (SMBs) and large cloud providers retain redundant data, in some cases for financial records or legal challenges. Inertia and legal concerns prevent a business from deleting a notable percentage of its data holdings. This has some governance and privacy implications for data protection principles, which are further developed in the next section. From a legal angle, the mere requirements to comply with policy requirements and adapt to evolving policies and procedures after the fact might prove a futile endeavour in any service agreement. The legal landscape is far from certain, and perhaps any agreement may prove to be illusory if new developments in technology or regulations occur (Akhtar et al., 2021).

The processing of personal data is a contentious aspect of cloud computing services, as many countries and organisations grow increasingly concerned about the legal atmosphere and consequences of cloud computing. Cloud computing privacy risks arise when cloud service providers and other service participants acquire, use, and disclose consumers' personal data without the consumer's knowledge, whether by consent or by law. Concerns have been expressed about the gathering and analysis of social media data for purposes other than law enforcement or counterterrorism. One prominent privacy risk in the cloud includes data mining. Organisations can combine extensive social data with transaction histories, public records, and other personal information to generate highly accurate predictions—such as user tracking. Additionally, registering for a cloud service may create a permanent log revealing when a particular user accessed the site, authenticated themselves, and the files they opened, until deleted or stale.

This information alone can reveal a substantial amount about an individual's life and activities, particularly when combined with tracking information from other websites (He et al., 2020).

**7.1.b. Data Sovereignty and Jurisdictional Issues**

Data sovereignty, linked to data privacy, focuses on where data is located and the applicable laws and regulations based on its geographical storage. This adds another layer of complexity for multinational companies in their data management strategies across multiple jurisdictions. As businesses and organisations operate across nations and regions, their data is inherently also subject to multiple legal systems. However, contrasting sets of regulations from different nations might sometimes lead to conflicting laws, which may have implications for international business operations. The development of high-tech products and vast networks will impact traditional business environments and open up a whole new area for the analysis of forensic cases. (Levinson et al., 2024).

Businesses and organisations operating across multiple nations face complex data sovereignty challenges. To ensure compliance with diverse data protection laws and regulations, these entities must navigate the intricate intersection of law and technology. By understanding the specific requirements of each jurisdiction and implementing robust data protection strategies, organisations can maintain their commercial structures while safeguarding sensitive information. Data stored in the cloud will be regulated or influenced by the law of the country in which the data centre is located (Kushwaha et al., 2020). Even when a company is headquartered in Country A, if its data is stored in Country B, issues of access and control will be regulated by the laws of Country B. Major cloud providers have distributed cloud data centres across dozens of locations to ensure high availability and disaster recovery options. The 'transborder data flow' principle is equally addressed by the cloud provider; who typical inform clients where their data is stored. Additionally, many providers offer clients the option to select a specific data storage region, based on business policies like 'data residency' or 'data sovereignty' concerns. These policies cater to local laws that strictly regulate data movement across international borders.

Cloud providers also commit to notifying organisations when governmental agencies request access to data stored in their data centres, provided if it aligns with the provider’s policies. It is incumbent upon the client organisation to be aware of and determine the local laws governing their overseas data centre contracts and that they comply in relation to either data transfer or access requests. If a local law enforcement agency has a legal right, it will still access the data, and the cloud provider will likely provide the client with the maximum available notice prior to access (Kushwaha et al., 2020).

## 8. Conclusion

Cloud security requires ongoing measures such as data encryption, strong access controls, application security testing, container security, and regulatory compliance. Organizations must continually adapt their security strategies to new technologies and evolving cyber threats. Therefore, it is critical to maintain the security posture by staying updated on threats and vulnerabilities and engaging qualified security personnel. Organisations prioritising cloud security can protect data, reduce risks, and build client trust, which is essential in today’s interconnected, cyber-vulnerable environment.

## References

1. Ahmad, S., Mehfuz, S., & Beg, J. (2022). Assessment on potential security threats and introducing novel data security model in cloud environment. Materials Today: Proceedings, 62, 4909-4915. https://doi.org/10.1016/j.matpr.2022.03.536

2. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16. https://doi.org/10.3390/electronics11010016
3. Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science Engineering and Technology.
4. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-Rimy, B. A. S. (2021). Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences, 11(19), 9005. https://doi.org/10.3390/app11199005
5. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. Ieee Access, 9, 57792-57807. DOI: 10.1109/ACCESS.2021.3073203
6. Apeh, A. J., Hassan, A. O., Oyewole, O. O., Fakeyede, O. G., Okeleke, P. A., & Adaramodu, O. R. (2023). GRC strategies in modern cloud infrastructures: a review of compliance challenges. Computer Science & IT Research Journal, 4(2), 111-125. https://doi.org/10.51594/csitrj.v4i2.609
7. Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 3(1), 242-251. DOI: 10.47709/ijmdsa.v2i2.3452
8. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
9. Bhadouria, A. S. (2022). Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. Int. J. Sci. Res. Publ. DOI: 10.29322/IJSRP.X.2022.p091095
10. Biswas, A., & Talukdar, W. (2023). Guardrails for trust, safety, and ethical development and deployment of Large Language Models (LLM). Journal of Science & Technology, 4(6), 55-82. https://doi.org/10.55662/JST.2023.4605
11. Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. Symmetry, 12(7), 1191. https://doi.org/10.3390/sym12071191
12. Casalicchio, E., & Iannucci, S. (2020). The state-of-the-art in container technologies: Application, orchestration and security. Concurrency and Computation: Practice and Experience, 32(17), e5668. https://doi.org/10.1002/cpe.5668
13. Chinamanagonda, S. (2022). Zero Trust Security Models in Cloud Infrastructure-Adoption of zero-trust principles for enhanced security. Academia Nexus Journal, 1(2).
14. Chirra, D. R. (2020). AI-Based Real-Time Security Monitoring for Cloud-Native Applications in Hybrid Cloud Environments. Revista de Inteligencia Artificial en Medicina, 11(1), 382-402. https://redcrevistas.com/index.php/RevistaPage
15. Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. International Journal of Production Research, 59(11), 3430-3445. https://doi.org/10.1080/00207543.2021.1884311
16. Daniel Croft. (2023). Tesla blames 2 former staff for data breach affecting 75k. https://www.cyberdaily.au/security/9459-tesla-blames-two-former-staff-for-data-breach-affecting-75k

17. David, D. S., Anam, M., Kaliappan, C., Selvi, S., Sharma, D. K., Dadheech, P., & Sengan, S. (2022). Cloud Security Service for Identifying Unauthorized User Behaviour. Computers, Materials & Continua, 70(2). DOI:10.32604/cmc.2022.020213
18. Deng, S., Zhao, H., Huang, B., Zhang, C., Chen, F., Deng, Y., ... & Zomaya, A. Y. (2024). Cloud-native computing: A survey from the perspective of services. Proceedings of the IEEE. DOI: 10.1109/JPROC.2024.3353855
19. Gao, J., Wang, H., & Shen, H. (2020, August). Machine learning based workload prediction in cloud computing. In 2020 29th international conference on computer communications and networks (ICCCN) (pp. 1-9). IEEE. DOI: 10.1109/ICCCN49398.2020.9209730
20. Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. (2022). Adoption of cloud computing as innovation in the organization. International Journal of Engineering Business Management, 14, 18479790221093992. https://doi.org/10.1177/18479790221093992
21. Goswami, P., Faujdar, N., Debnath, S., Khan, A. K., & Singh, G. (2024). Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability. Journal of Cloud Computing, 13(1), 45. https://doi.org/10.1186/s13677-024-00605-z
22. Gupta, M., Awaysheh, F. M., Benson, J., Alazab, M., Patwa, F., & Sandhu, R. (2020). An attribute-based access control for cloud enabled industrial smart vehicles. IEEE Transactions on Industrial Informatics, 17(6), 4288-4297. DOI: 10.1109/TII.2020.3022759
23. He, Q., & He, H. (2020). A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining. Sustainability, 13(1), 101.
24. Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), 3587-3608. https://doi.org/10.1007/s11831-022-09708-9
25. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 129-171. https://doi.org/10.60087/jaigs.v2i1.102
26. Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, M. S., Watters, P. A., Ng, A., ... & Kumara, I. (2020). A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. Sensors, 20(9), 2464. https://doi.org/10.3390/s20092464
27. Kushwaha, N., Roguski, P., & Watson, B. W. (2020, May). Up in the air: Ensuring government data sovereignty in the cloud. In 2020 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 43-61). IEEE. DOI: 10.23919/CyCon49761.2020.9131718
28. Kushwaha, N., Roguski, P., & Watson, B. W. (2020, May). Up in the air: Ensuring government data sovereignty in the cloud. In 2020 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 43-61). IEEE. DOI: 10.23919/CyCon49761.2020.9131718
29. Levinson, M., Reid, E., O'Brien, S., & Geron, T. (Eds.). (2024). Civic Contestation in Global Education: Cases and Conversations in Educational Ethics. Bloomsbury Publishing.
30. Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. Journal of Management Information Systems, 38(1), 222-245. https://doi.org/10.1080/07421222.2021.1870390
31. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

32. Lindsay Shachnow. (2022). Uber Users: What You Need to Know about Last Month's Data Breach. https://www.bu.edu/articles/2022/what-you-need-to-know-about-uber-data-breach/
33. Maaz, M., Ahmed, M. A., Maqsood, M., & Soma, S. (2023). Development Of Service Deployment Models In Private Cloud. Journal of Scientific Research and Technology, 1-12. https://doi.org/10.61808/jsrt74
34. Mehraj, S., & Banday, M. T. (2020, January). Establishing a zero trust strategy in cloud computing environment. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE. DOI: 10.1109/ICCCI48352.2020.9104214
35. Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. Applied Sciences, 13(19), 10871. https://doi.org/10.3390/app131910871
36. Mustyala, A. (2023). Migrating Legacy Systems to Cloud-Native Architectures for Enhanced Fraud Detection in Fintech. EPH-International Journal of Science And Engineering, 9(1), 16-26. https://doi.org/10.53555/ephijse.v9i1.236
37. Oladoyinbo, T. O., Adebiyi, O. O., Ugonnia, J. C., Olaniyi, O., & Okunleye, O. J. (2023). Evaluating and establishing baseline security requirements in cloud computing: an enterprise risk management approach. Available at SSRN 4612909. http://dx.doi.org/10.2139/ssrn.4612909
38. Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114, 102580. https://doi.org/10.1016/j.cose.2021.102580
39. Patel, N. (2024). Secure Access Service Edge (SASE): Evaluating the impact of converged network security architectures in cloud computing. Journal of Emerging Technologies and Innovative Research, 11(3), 12.
40. Patil, K., Desai, B., Mehta, I., & Patil, A. (2023). A Contemporary Approach: Zero Trust Architecture for Cloud-Based Fintech Services. Innovative Computer Sciences Journal, 9(1). https://innovatesci-publishers.com/index.php/ICSJ/article/view/165
41. Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., & Karri, R. (2022, May). Asleep at the keyboard? assessing the security of github copilot's code contributions. In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 754-768). IEEE. DOI: 10.1109/SP46214.2022.9833571
42. Pero, V., & Ekman, L. (2023). Implementing a zero-trust environment for an existing on-premises cloud solution. URN: urn:nbn:se:kth:diva-328402
43. Rangnau, T., Buijtenen, R. V., Fransen, F., & Turkmen, F. (2020, October). Continuous security testing: A case study on integrating dynamic security testing tools in ci/cd pipelines. In 2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC) (pp. 145-154). IEEE. DOI: 10.1109/EDOC49727.2020.00026
44. Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021(1), 7608296. https://doi.org/10.1155/2021/7608296
45. Rice, L. (2020). Container security: Fundamental technology concepts that protect containerized applications. " O'Reilly Media, Inc.".
46. Said, W., Mostafa, E., Hassan, M. M., & Mostafa, A. M. (2022). A multi-factor authentication-based framework for identity management in cloud applications. CMC-Computers Materials & Continua, 71(2), 3193-3209. DOI:10.32604/cmc.2022.023554

47. Segun-Falade, O. D., Osundare, O. S., Kedi, W. E., Okeleke, P. A., Ijomah, T. I., & Abdul-Azeez, O. Y. (2024). Assessing the transformative impact of cloud computing on software deployment and management. Computer Science & IT Research Journal, 5(8). DOI: 10.51594/csitrj.v5i8.1492
48. Shakor, M. Y., Khaleel, M. I., Safran, M., Alfarhood, S., & Zhu, M. (2024). Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. IEEE Access. DOI: 10.1109/ACCESS.2024.3351119
49. Stafford, V. (2020). Zero trust architecture. NIST special publication, 800, 207. https://doi.org/10.6028/NIST.SP.800-207
50. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532. https://doi.org/10.1007/s11227-020-03213-1
51. Thabit, F., Alhomdy, S. A. H., Alahdal, A., & Jagtap, S. B. (2020). Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques. Journal of Information and Computational Science, 12(10). https://ssrn.com/abstract=3749271
52. Toyota Motor Corporation. (2023). Data breach and security incident report. Toyota Motor Corporation. https://global.toyota/en/newsroom/corporate/39241625.html
53. Vallabhaneni, R. (2024). Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices.
54. Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys (CSUR), 53(4), 1-41. https://doi.org/10.1145/3398036
55. Srinivasan, K., Kumar, M. R., & Elango, R. (2021). Cloud computing and its impact on modern businesses. Journal of Business and Cloud Computing, 14(3), 45-60. https://doi.org/10.1016/j.jbcc.2021.03.014
56. Sharma, R., & Gupta, P. (2022). Trends in cloud adoption: A shift to scalable infrastructures. Cloud Computing Insights, 11(2), 123-139. https://doi.org/10.1109/CCI.2022.9832110
57. Ahmed, T., Khan, A., & Rahman, F. (2023). Benefits of cloud environments: An organisational perspective. Cloud and Data Security Review, 9(1), 1-12. https://doi.org/10.1016/j.cdsc.2023.02.008
58. Cybersecurity Ventures. (2022). Cloud attack vectors and their implications. Retrieved from https://www.cybersecurityventures.com/reports/cloud2022
59. Smith, J., Rogers, K., & Patel, N. (2023). Vulnerability analysis in cloud environments. Journal of Cybersecurity, 18(4), 345-361. https://doi.org/10.1080/2333341.2023.093332
60. Miller, D., & Jones, A. (2020). Reactive versus proactive cloud security strategies. Cybersecurity Trends, 7(5), 202-214. https://doi.org/10.1007/s10233-020-07711
61. Gupta, M., Benson, J., & Alazab, M. (2020). An attribute-based access control for cloud-enabled industrial smart vehicles. IEEE Transactions on Industrial Informatics, 17(6), 4288-4297. https://doi.org/10.1109/TII.2020.3022759
62. Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., & Karri, R. (2022). Security integration in software development. IEEE Symposium on Security and Privacy, 12(5), 754-768. https://doi.org/10.1109/SP46214.2022.9833571
63. Casalicchio, E., & Iannucci, S. (2020). The state of the art in container technologies: Application, orchestration and security. Concurrency and Computation: Practice and Experience, 32(17), e5668. https://doi.org/10.1002/cpe.5668

64. Li, H., Yoo, S., & Kettinger, W. J. (2021). Roles of IT strategies and security investments in reducing organisational breaches. Journal of Management Information Systems, 38(1), 222-245. https://doi.org/10.1080/07421222.2021.1870390
65. Pero, V., & Ekman, L. (2023). Implementing a zero-trust environment for an existing on-premises cloud solution. URN: KTH Reports. https://doi.org/10.23919/CyCon49761.2020.9131718
66. He, Q., & He, H. (2020). Enhancing security in cloud computing. Sustainability, 13(1), 101. https://doi.org/10.3390/su13010101
67. Kushwaha, N., Roguski, P., & Watson, B. W. (2020). Data sovereignty in the cloud. Cyber Conflict Proceedings, 12(5), 43-61. https://doi.org/10.23919/CyCon49761.2020.9131718