Evaluating Advanced Cybersecurity Technologies for Cloud Environments

Nirmal Kavindu Athukorale , Chua Jing Yi , Loh Zi Xin , Alysha Yasmine , Choo Jia Qi , Dang Zi Yu , Jason Soo Jia Wei , Filbert Hady , Lim Shi Zhe , Chua Chong Eu , Siva Raja Sindiramutty *

Posted Date: 6 January 2025

doi: 10.20944/preprints202501.0395.v1

Keywords: cloud security; cybersecurity frameworks; data encryption; threat detection; hybrid cloud solutions

Article

Evaluating Advanced Cybersecurity Technologies for Cloud Environments

Nirmal Kavindu Athukorale, Chua Jing Yi, Loh Zi Xin, Alysha Yasmine, Choo Jia Qi, Dang Zi Yu, Jason Soo Jia Wei, Filbert Hady, Lim Shi Zhe, Chua Chong Eu and Siva Raja Sindiramutty *

Taylor's University, Malaysia

* Correspondence: magan.shiva91@gmail.com (S.R.S.)

Abstract: This paper addresses the rise of cyberattacks that pose significant threats to computer and network systems, including data breaches, malware, and unauthorized access, which are becoming increasingly prevalent (Aslan et al., 2023). It explores how security measures in cloud computing protect sensitive data and ensure operational integrity as more organizations adopt cloud environments. The paper examines advanced cloud security technologies concerning their mechanisms, components, and role in addressing modern cybersecurity challenges. Key elements such as data encryption, network security, and auditing are discussed regarding their role in safeguarding sensitive information within cloud environments. Essential processes such as identifying, protecting, detecting, responding, and recovering are considered in developing a comprehensive cybersecurity framework for cloud systems. Besides that, the paper also evaluates examples of advanced cloud security measures, such as encryption technologies, and discusses their benefits, including multi-layered defence, scalability, and cost efficiency. The presented limitations, which involve compliance challenges, multi-tenancy risks, and reduced direct control are critically assessed. Furthermore, the paper discusses future directions in cloud security, including edge-cloud computing and hybrid cloud solutions. Finally, it proposes advanced countermeasures, such as intelligent deception technologies using honeytokens and honeynets to dynamically mitigate evolving threats. This study emphasizes the importance of adaptive and proactive strategies for cloud environment security as well as provides valuable insights relevant to both academic research and practical implementation.

Keywords: cloud security; cybersecurity frameworks; data encryption; threat detection; hybrid cloud solutions

1. Background

Introduction to Cloud Computing Security

Cloud computing security, commonly called cloud security, encompasses a variety of technologies, procedures, and practices used to secure cloud-based infrastructures, data, and applications against cyber threats. As businesses across the globe move to cloud platforms to support their data storage and application needs, establishing reliable cloud security has become essential (Ananna et al., 2023). Cloud security aims to protect the privacy of data, whilst complying with regulations, and ensure the integrity of cloud-stored information. Commonly used security techniques include encryption, identity and access management (IAM), and ongoing threat detection to prevent unauthorised access and safeguard data (Google Cloud, n.d; Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023).

One of the key elements of cloud security is called the shared responsibility model, which assigns specific security roles to both the provider of the cloud service and the customer. The

 doi:10.20944/preprints202501.0395.v1

providers are responsible for the security of the physical infrastructure and data centre environments, while customers handle the security of data, user access, and settings within the applications they deploy on the cloud. For effective protection, it's critical that both parties clearly understand and manage their roles to prevent any potential security gaps (IBM, 2024).

The Importance of Cloud Security

Cloud security has become increasingly significant as organisations in fields such as healthcare, finance, and retail industries that often manage sensitive information shift to cloud-based environments. Ensuring data protection is essential to prevent breaches and data losses, as well as to stay in compliance with legal standards like the General Data Protection Regulation, aka. GDPR and the Health Insurance Portability and Accountability Act, better known as HIPAA. Organisations with healthy cloud security practices not only reduce the risk of severe penalties for non-compliance but also safeguard their reputation (Kaspersky, 2020; Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023).

Beyond compliance, cloud security is crucial for maintaining business continuity. By implementing secure backups, disaster recovery solutions, and robust access controls, companies reduce the risk of operational downtime following a security breach. This resilience allows businesses to quickly restore operations and ensure customer satisfaction, making cloud security an essential element in risk management strategies (Google Cloud, n.d.)

Challenges in Cloud Computing Security

Despite its benefits, cloud computing poses significant security challenges because of the open and complex nature of cloud environments. One major concern is data breaches and loss. The shared infrastructure of cloud services makes them particularly vulnerable to breaches, which can result in serious damage to both financial stability and reputational trust. According to the Cost of a Data Breach Report from IBM, the financial impact of a data breach, on average, has exceeded $4 million, underscoring the need for robust security protocols and constant vigilance to protect sensitive information (IBM, 2024; Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023).

Another critical issue involves insecure APIs and interfaces. APIs are integral to enabling interactions between applications in cloud environments, but poorly secured APIs can create vulnerabilities (Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023; Hussain et al., 2024). To mitigate this risk, organizations must adopt secure coding practices and implement strong access controls, ensuring APIs do not become gateways for unauthorized access or data breaches (Google Cloud, n.d.). Account hijacking and unauthorized access further complicate cloud security. Cybercriminals often exploit phishing attacks and malware to steal user credentials, enabling them to gain access to cloud resources unlawfully. Implementing multi-factor authentication (MFA) and strict identity and access management (IAM) policies is essential to minimize this risk and ensure sensitive data and applications can only be accessed by personnel who are authorized (Kaspersky, 2020; Jun et al., 2024).

Finally, compliance and regulatory challenges present another layer of complexity. Cloud users must navigate diverse regulatory frameworks across different regions, ensuring they comply with standards such as GDPR and HIPAA. This task is particularly resource-intensive and challenging for companies operating across multiple jurisdictions, requiring significant effort to maintain compliance while managing cloud-based operations (IBM, 2024).

2. Discussion on How Security-Related Technology Works

a) Component

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 January 2025 doi:10.20944/preprints202501.0395.v1

Cloud computing security involves various components designed to protect our data, applications, and infrastructure in the cloud. Here are some essential components of cloud computing security:

i. Data Encryption

Data encryption permits data to be protected in the course of storage and during transfer from one system to another. Encryption in cloud computing involves storage encryption by means of AES-256 and data transferred over a network using Transport Layer Security (Shanshan et al., 2023; Aljabri et al., 2021; Manchuri et al., 2024). This helps in maintaining privacy and sanity of data, by avoiding compromise from external or even internal vandals. Figure 1 shows how the conventional encryption works.

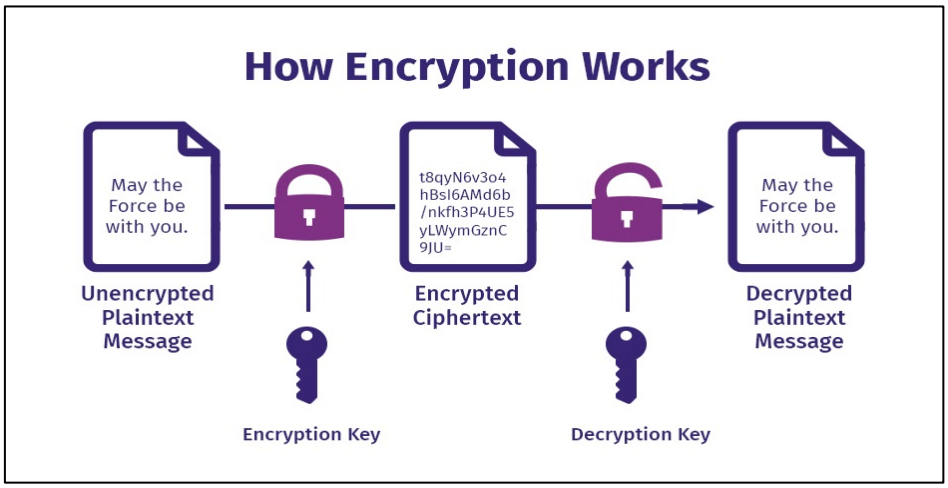

Figure 1. How Encryption Works (Dutta, 2024).

Types of Encryption

- Encryption at Rest: This implies that data is stored encrypted when not in use. Cloud providers use strong encryption standards like AES-256 to restrict unauthorized access to data.
- Encryption in Transit: Information moving between the customer's device and the cloud-including from one cloud to another is encrypted using Transport Layer Security, and Secure Sockets Layer.
- Encryption in Use: In an emerging area like this, data is made incomprehensible when it is in use. For example, Homomorphic encryption enables computations on plain text data while it is still encrypted.

Key Management

Encryption is only as secure as its keys. Key Management Services(KMS) allow organizations to securely generate, store, rotate and control access to their encryption keys. KMS is very often set up with integrations to cloud platforms for automation of encryption and key management. BYOK stands for Bring Your Own Key; many organizations prefer this method as a way to manage their own keys on the cloud. This adds a layer of control and ensures no third-party access to keys.

ii. Network Security

Firewalls deployed in cloud settings perform the same role as the physical firewalls located on-premises—they regulate access to and out of the cloud resources by allowing or blocking ingress and egress traffic respectively. These may be in the form of software firewalls or even virtual appliances based within the cloud

 doi:10.20944/preprints202501.0395.v1

architecture like IDS/IPS.(Tu et al., 2023; NIST SP 500-292, 2011; Ravichandran et al., 2024)

Firewalls Features

- Network-based Firewalls: Secure the perimeters of a cloud network by managing the flow of traffic based on certain IP addresses, ports or protocols. They apply the policies uniformly across the virtual private clouds (VPCs) and subnetworks. (Reddy, 2023)
- Web Application Firewalls (WAF): These firewalls are aimed at preventing attacks on web applications, which are the most common forms like SQL Injection and Distributed Denial of Service (DDoS) attacks by thorough checking of the HTTP requests.

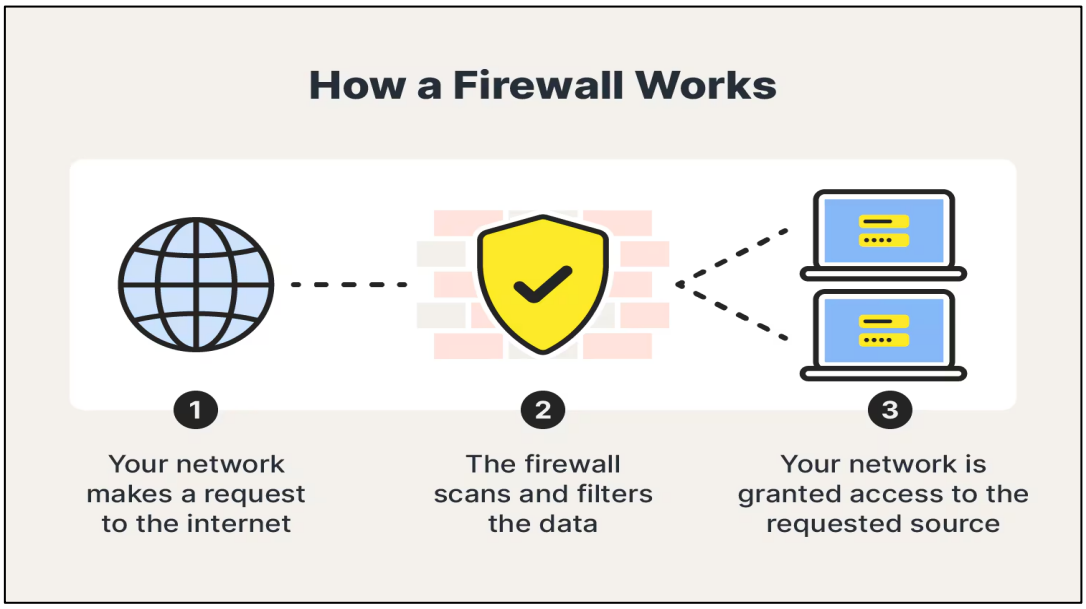

Figure 2. How a Firewall Works (Chebitko, 2024).

How It Works

- The way cloud firewalls work is by setting up security groups or by setting up network access control lists (ACLs). These include rules which state what traffic is permitted and what traffic is denied.
- Intrusion Detection/Prevention Systems (IDS/IPS): This is frequently done in combination with firewalls as a mechanism to inform and help the administrators of the network of the threat in real-time and even block any traffic that appears to be malicious traffic.

iii. Auditing

Auditing is a decisive aspect of cloud security which upholds responsibility and honesty and promotes adherence to rules within the cloud context. It encompasses the practice of reviewing and analyzing processes and/or activities carried out in the cloud to uncover security threats, risks, or breaches. This proposition gives control back to the organizations in terms of managing their data and infrastructure on the cloud.

Key Concepts

- Data Integrity and Compliance: Auditing acts to ensure that data is preserved without modifications and assists organizations in meeting laws such as GDPR and HIPAA. (Shanshan et al., 2023; Seng et al., 2024).
- Event Logging: Important activities such as data entry and retrieval, modification of settings, and user logins are documented in order to leave a clear trace of the activities performed.

How It Works

 doi:10.20944/preprints202501.0395.v1

To investigate the system for any malpractices or unusual patterns, systems demonstrate and, very often, automatically check for violations using set user actions and other system hints. Similarly, logging is embedded into the mechanisms of the cloud services such as AWS and its AWS CloudTrail service, which captures calls made to the application programming interface (API) and their use in evaluating the security of the system by the auditors.

iv. Authentication and Access Control

This is very important in terms of enabling control over who has access to cloud resources and the ability to conduct any action on them. It ensures that authenticated users or systems have access to only authorized sensitive data and services residing within the cloud.

Key Concepts:

- Authentication: It ensures the verification of a user in order to assert who he/she claims to be. In Cloud environments, this generally includes Passwords, Multi-factor authentication MFA, Biometric Verification (thumb impressions, facial recognition) and SSO - Single Sign-On. (Shanshan et al., 2023; Mbah, 2022)
- Authorization: This is what the user can do once they are authenticated. In most scenarios, this is done through roles and permissions. A good example is when admins have full permissions, whereas normal users will have very limited permissions.
- Role-Based Access Control (RBAC): A very applicable feature today; it is a system where permissions are granted through roles, not to the individual users themselves. This will help in managing a great number of user accesses efficiently.

How It Works

IAM functions at the user, group, or service level based on access policies and roles. Policies can normally be written in JSON to outline which actions could be performed, written, or deleted against which resources should be allowed or denied. It also integrates with multi-factor authentication (MFA) for additional layers of security. (Shanshan et al., 2023; Mbah, 2022; Sindiramutty et al., 2024)

b) Process

The National Institute of Standards and Technology has cybersecurity standards that claim, a structured plan to manage the risk of cyberattacks can be established through five main pillars, which are to identify, protect, detect, respond and recover. Together, these pillars can provide a thorough framework that ensures a strong and complete approach to cybersecurity, covering all essential aspects of security management and resilience (NIST, 2018; Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024).

v. Identify

Based on (NIST, 2018), the identify function helps an organisation establish a thorough understanding of managing risks in cybersecurity across its systems, data, people, assets and capabilities. The resources that are essential to critical operations, and associated cybersecurity risks, an organisation can align its priorities and efforts effectively with its risk management strategy and business goals, by understanding the business context. In cloud security, the identified function can involve documenting assets such as virtual machines, containers, data storage instances, applications, and user roles across the cloud infrastructure (Practical Cloud Security A Guide for Secure Design and Deployment, n.d.). By doing so, organizations can understand what needs protection, and identify interdependencies within the cloud, and assess vulnerabilities that could be exploited (Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024). Apart from that, risk assessments and data classification are also the key components in this process, which enable organisations to prioritise security measures based on the sensitivity of different cloud assets.

To perform the identified function in cloud security, organisations can use various tools to gain visibility into their cloud environment and assess risks. For example, Cloud Workload Protection

 doi:10.20944/preprints202501.0395.v1

Platforms and Vulnerability Assessment Tools can be used to identify risks within workloads and configurations, while Cloud Security Posture Management Tools can identify risks from misconfigurations, policy violations, and security weaknesses across different cloud components by continuously monitoring and evaluating cloud environments (Kunduru, 2023). Together, these tools provide a comprehensive view of assets and risks, supporting effective security management in the cloud.

vi. Protect

The Protect function involves a range of security measures designed to ensure that critical infrastructure can withstand potential attacks while maintaining data confidentiality, integrity, and availability (NIST, 2018; Sindiramutty et al., 2024). One of the key measures to achieve protection in cloud security is Encryption Technologies, which protect sensitive information, both at rest and in transit from unauthorised access (Blessing, 2024). Using encryption key management systems (KMS), organisations can securely manage and store encryption keys, providing essential data assets with a higher level of protection. Additionally, by requiring multiple forms of identification, the integration of Multi-Factor Authentication (MFA) with Identity and Access Management (IAM), strengthens user verification, and substantially reduces the risk of access that may be unauthorised (Ul Haq and Sharma, 2023). Furthermore, Firewalls and Intrusion Prevention Systems (IPS) also serve as further protective measures to secure cloud resources from malicious traffic (Kunduru, 2023). Through the established rules and active prevention of potential threats, these systems can block unauthorised access, reinforcing the security of cloud environments against external attacks. Together, these protections work to create a strong foundation that helps organisations protect their cloud infrastructure against threats.

vii. Detect

The Detect function from the five main pillars of cybersecurity standards focuses on identifying cybersecurity events and anomalies as early as possible and helping organisations respond to potential incidents quickly (NIST, 2018). Cloud security involves monitoring network traffic, application behaviour, and user activities within the cloud environment for signs of unusual or unauthorised actions. For example, Intrusion Detection Systems (IDS) are one of the essential tools for cloud detection, as they continuously analyse network traffic, both outgoing and incoming, to alert security teams to suspicious activity that could indicate a potential attack (Lata and Singh, 2022; Sindiramutty, Tan, Shah, et al., 2024). Additionally, Security Information and Event Management (SIEM) tools are another core component, which aggregates and analyses log data from many sources, like applications, databases, and user access logs, across the cloud infrastructure (Kunduru, 2023; Sindiramutty, Tan, & Wei, 2024). Apart from that, SIEM solutions enable security teams to detect patterns and correlate events that may reveal advanced threats or breaches while Threat Intelligence platforms and Behavioral Analytics often leverage AI to identify emerging risks and unusual behaviours, tracking anomalies in user activities and detecting potential insider threats. Combining these detection capabilities, organisations can maintain visibility into cloud activities and support proactive identification and resolution of security issues.

viii. Response

The Response Function is the specific actions done to effectively address a cybersecurity incident that has been detected. According to (NIST, 2018), it enables organisations to reduce the possible impact of a cybersecurity incident. In cloud security, this involves implementing response protocols tailored to the cloud environment and integrating cloud-specific Incident Response Plans with automated tools for real-time containment. SIEM Integration with automated incident response solutions plays a critical role, allowing organisations to quickly identify threats and initiate containment measures, such as separating affected resources or blocking IP addresses that are

 doi:10.20944/preprints202501.0395.v1

deemed malicious (Waheed et al., 2024). Other than that, Intrusion Prevention Systems (IPS), which are often built into cloud environments, can contribute by blocking suspicious traffic and limiting the spread of an incident in real-time. Policy Enforcement mechanisms and Data Loss Prevention (DLP) systems also offer additional layers of automated response, which detect policy violations, such as unauthorised data transfers, and alert administrators while containing potential data leaks (Brown, 2024). Security teams can respond quickly and effectively by implementing these response mechanisms, to reduce the impact on resources and operations.

ix. Recover

The Recover Function, as outlined by NIST (2018), includes activities aimed at maintaining resilience and restoring disrupted capabilities or services after a cybersecurity incident. It enables a prompt return to its usual operations to reduce the impact of the incident. For example, backup and disaster recovery solutions enable automated, frequent data backups, allowing rapid data restoration when the data is lost or damaged. Disaster Recovery as a Service (DRaaS) enhances this by replicating applications and data in real-time across multiple geographic regions, allowing for rapid failover and restoration of functionality after a disruption. The flexible recovery points and recovery time objectives (RPOs and RTOs) supported by DRaaS help organisations maintain operational continuity even in large-scale incidents (Sheriffdeen, 2022; Wen et al., 2023). Additionally, Patch Management is an important component of recovery in cloud environments. By regularly applying security patches and updates to applications, virtual machines, and other resources, organisations reduce vulnerabilities that could otherwise be exploited in future incidents (Chauhan and Shiaeles, 2023). These recovery strategies have ensured the resilience of cloud infrastructure, enabling organisations to restore functionality swiftly and prevent prolonged business impacts from cybersecurity events.

c) Threats

There are a large number of increasingly complex threats faced in cloud security environments. These threats not only pose risks to companies' sensitive data but also affect the security of overall business operations. This section will focus on data leaks, malware and ransomware, service outages, as well as account hijacking challenges.

First of all, considering the immense data companies store in the cloud while facing safety hazards in transferring across networks, data leaks are considered one of the most critical threats in cloud environments. They typically occur due to insecure APIs that lack proper verification and protection, allowing attackers to easily access and even tamper with confidential information. Configuration errors and user negligence also contribute to data leaks. In January 2023, T-Mobile experienced a data leak, and 37 million users were affected. The data including the user's personal information like email addresses, phone numbers, and names, were accessed by attackers through an API vulnerability. Although T-Mobile stated that payment information and Social Security numbers were not compromised (Krebs, 2023; Alex et al., 2022), the exposure of client data still impacts the company's reputation and economy.

Furthermore, as more companies migrate their data and systems to the cloud, attacks from malware and ransomware in cloud environments are constantly increasing, damaging cloud security. Attackers normally exploit phishing emails and social engineering techniques to lure users into installing malicious software, allowing them to target the key server information. A notable example is in May 2021 when Colonial Pipeline suffered a ransomware attack due to an unused VPN account being exploited by hackers, leading the company to pay a ransom of $4.4 million (Jack Beerman, et al., 2023; Alferidah & Jhanjhi, 2020). Nowadays, the advent of Ransomware-as-a-Service (Raas) has enabled large-scale attacks, even by relatively low-skilled hackers (Amos Kibet, et al., 2022). In other words, companies face the dual risks of data being locked and the difficult decision-making between paying the ransom or attempting to recover their data.

Cloud service outages are a grave menace that can significantly impact companies' operations. Denial of Service (DoS) attacks send large numbers of false requests, overloading cloud infrastructure

 doi:10.20944/preprints202501.0395.v1

and causing services to slow down or even interrupt. Since even a single cloud server being attacked can implicate many other users, this attack method is especially dangerous in cloud environments. When workloads increase, cloud systems automatically deploy new virtual machines and service instances to provide additional computing resources, but this also creates potential vulnerabilities in cloud environments. In Distributed Denial of Service (DDoS) attacks, attackers might be able to control multiple devices by exploiting botnets to raise attacks on systems, further intensifying the cloud environment burden. In February 2018, GitHub experienced DDoS attacks with a peak value reaching 1.35 Tbps. Using Memcached amplification from over 51,000 vulnerable servers, vast amounts of traffic flooded the servers in a short time (Kumar, 2018; Alkinani et al., 2021), leading to outages and affecting global user accessibility. These outages highlight the weaknesses within cloud environments and are regarded as critical examples of the threat to cloud security.

Moreover, account hijacking cases are growing incessantly in cloud environments. Hackers gain user credentials and control cloud accounts, which could lead to privacy data loss and service abuse. Attack actions not only come from outsiders, even insiders might exploit access permissions to conduct malicious activities. Insiders Threat Report reveals that 74% of cybersecurity experts stated that the frequency of insider threats has risen within the past year. As more companies use cloud services, 53% of interviewees indicated that detection of this attack method has become more difficult (Schulze, 2023; Babbar et al., 2021). In the 2019 Capital One data breach case, an engineer of Amazon Web Services engineer leveraged a Web Application Firewall that was misconfigured, to get unauthorized access to sensitive information from over 100 million clients. (Gurulcu, 2023). This illustrates how insiders and account hijacking create burdens for cloud environments. Outsiders might also employ means to hijack accounts, including remote attacks on cloud infrastructure and applications, and even attacks on cloud user endpoints.

In short, the issues mentioned above can significantly affect companies and user privacy, constituting major threats to cloud security. Companies must adopt a comprehensive approach, like improving API protection enhancing user security awareness and ensuring adherence to data protection legislation to lower the risk of getting the data breached and privacy violations.

d) Example security-related technology

x. Data Encryption Technologies

Data encryption is a key method to keep data safe in cloud environments. By using encryption, data is protected both when stored and during transmission, which helps prevent unauthorized access and data leaks. (Wang.Z.Y,2020; Brohi et al., 2020). Some common encryption methods used in cloud computing include symmetric encryption, asymmetric encryption, homomorphic encryption, and attribute-based encryption.

Symmetric Encryption

In symmetric encryption, the same key is used in the encryption and decryption of data. It is fast and effective, making it perfect for securing huge amounts of data. The encryption and decryption processes are the reverse of each other.

Encryption: C=E(K,P)

Decryption: P=D(K,C)

Where:

P = Plaintext (original data) C = Ciphertext (encrypted data)

K = Key (used for both processes) E = Encryption function

D = Decryption function

 doi:10.20944/preprints202501.0395.v1

Common symmetric encryption algorithms are **AES** (Advanced Encryption Standard) and **DES** (Data Encryption Standard).

Asymmetric Encryption

Asymmetric encryption, or public key encryption, makes use of two keys: a public and a private key. The public key is used to encrypt the data, and the private key decrypts it. This method is used for key management and is especially effective for secure data transfer in cloud systems.

Encryption: C=E(Kpub,P)

Decryption: P=D(Kpri,C)

Where:

Kpub = Public key Kpri = Private key P = Plaintext C = Ciphertext

RSA and ECC (Elliptic Curve Cryptography) are two popular asymmetric encryption techniques.

Homomorphic Encryption

Homomorphic encryption enables calculations, like multiplication and addition, to be done on encrypted data without it having to be decrypted first. This is particularly useful for cloud services, as it allows sensitive data to be processed while remaining encrypted, ensuring privacy.

Attribute-Based Encryption (ABE)

ABE encrypts data based on specific user attributes (like role, location, etc.), and decryption is allowed only for users who meet the access policy defined by those attributes. There are two main types of ABE: Key-Policy ABE and Ciphertext-Policy ABE.

Encryption: C=E(PK,P,A)

Decryption: P=D(SK, C)

Where:

PK = Public key SK = User's private key

P = Plaintext C = Ciphertext

A = Access policy

3. Discussion on the Impact

i. Benefits

a) Multi-Layered Defence

Cloud security also provides a multi-layered defence for data protection. Data in a cloud environment can be classified into three states, Data at Rest, Data in Motion, and Data in Use. When data is at rest, the cloud intrusion detection system (IDS) in the cloud environment encrypts and scans for any suspicious data. When the data is in Motion (in transit) IDS protects data against leaks in the cloud environment so that sensitive data is secure during transmission. When data is in Use, cloud IDS tracks data accessed by peripherals, reducing the risk of unauthorized transfers, especially in situations when physical ends can be the point of leakage. Cloud security ensures that the data is always encrypted and access controls restrict the user's permission to view or modify the data to reduce the risk of unauthorized access (Chesti et al., 2020). Cloud IDS also uses encryption methods such as elliptic curve cryptography to authenticate devices before they access cloud resources, minimizing the risk of data leaks to unverified devices. (Alouffi, B., et al. 2021; Dogra et al., 2021).

 doi:10.20944/preprints202501.0395.v1

b) Scalability

Scalability is a key advantage of cloud security. This feature allows users to scale the security resource based on fluctuating demand, without the need for costly new hardware or infrastructure investments and installation complexity. In a cloud environment, security resources and protocols automatically scale in line with the workload, ensuring consistent protection regardless of the changes in demand. This is particularly beneficial in the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) models, where cloud service providers (CSP) like AWS, Google Cloud, or Azure handle the underlying infrastructure and support dynamic scaling. When facing increasing data traffic, CSPs can scale their server capacity to meet this demand, while maintaining secure access controls and threat defence. Companies get to avoid disruptions and ensure the data in the cloud environment is secure and stable while keeping the cost manageable during high-traffic periods. (Rashid, A. and Chaturvedi, A., 2019; Fatima-Tuz-Zahra et al., 2020).

c) Cost Saving

A major advantage of cloud security is the significant cost savings it offers by eliminating the need for organizations to invest in physical security infrastructure or maintain dedicated IT staff specifically for security management. In a traditional setup, businesses would need to purchase costly hardware like firewalls, intrusion detection systems, and secure servers. Additionally, they would need to regularly upgrade this equipment to stay current, along with hiring skilled IT staff to monitor, maintain, and troubleshoot these systems. For cloud security, cloud service providers such as Amazon AWS, Microsoft Azure, and Google Cloud offer security services that are built into their platforms, including firewalls, encryption, and compliance tools. The cost for maintenance of infrastructures and IT manpower can be reduced significantly as the CSP will handle it. Automatic updates are also provided by CSP as routine maintenance and patching are done regularly to ensure the security resources are up to date to prevent outdated security patches from known exploits. (Kumar, G., 2019; Gopi et al., 2021)

ii. Limitations

a) Limited Direct Control

Due to the asymmetry in access and control between client organizations and cloud service providers, cloud computing can present various limitations in terms of security. Cloud service providers like Amazon Web Service(AWS), Microsoft Azure and Google Cloud Platform(GCP) will have full control over security, leading to the primary security objective in cloud computing, which is limited direct control over the client organization (Tabrizchi and Rafsanjani, 2020). Cloud service providers will control the platform's frontend architecture and backend infrastructure (AlTwaijiry, 2021; Gouda et al., 2022) while the client organization will only have limited visibility and influence over data management and application security.

b) Compliance and Regulatory Challenges

In addition, compliance and regulations are the limitations that must unavoidably be faced in cloud environments. With the global increase in legislations for data protection such as GDPR, HIPAA and CCPA, companies must make sure that their cloud services comply with each country's laws and regulations (Tisha Garg, et al., 2024; Humayun et al., 2022). This involves implementing technical security measures and comprehensive regulation and data management practices. In 2023, the Irish Data Protection Commission fined Meta, 1.2 billion euros based on EDPB finding for illegally transmitting user data to the USA thereby violating GDPR (EDPB, 2023). This case emphasizes the importance of ensuring compliance in data transfers to protect user privacy and reduce cases of data breaches.

 doi:10.20944/preprints202501.0395.v1

c) Multi-Tenancy Risk

Moreover, risk from multi-tenancy is another limitation of the cloud computing environment. Multi-tenancy is a fundamental concept of cloud computing where many users or tenants share the same computing resources such as servers, storage, and networking while they are sandboxed from their environment. (Hashim and Noor, 2024; Jhanjhi et al., 2021). It is cost-effective for both provider and customer aspects as the cost of maintaining and updating hardware is shared among all users. However, isolation failures will be the weaknesses of multiple tenant cloud environments since they will also create an opportunity for intruders to conduct data breaches. As an illustration, an attacker has been able to "escape" from their virtual machines and access data in another VM that operates on the same physical server due to flaws in hypervisors. (Hashim and Noor, 2024; Kumar et al., 2021).

iii. Future Potentials

a. Edge-Cloud Computing

Despite the powerful capabilities of cloud computing, communication latency and increased security risks can be caused due to long distances between terminal devices and remote servers and limited bandwidth (AlTwaijiry, 2021; Lim et al., 2019). To address these challenges, edge computing emerges as a solution by combining centralized cloud servers with distributed edge servers near terminal devices, which helps to reduce latency by processing and storing data at multiple locations along the path, as shown in Figure 3

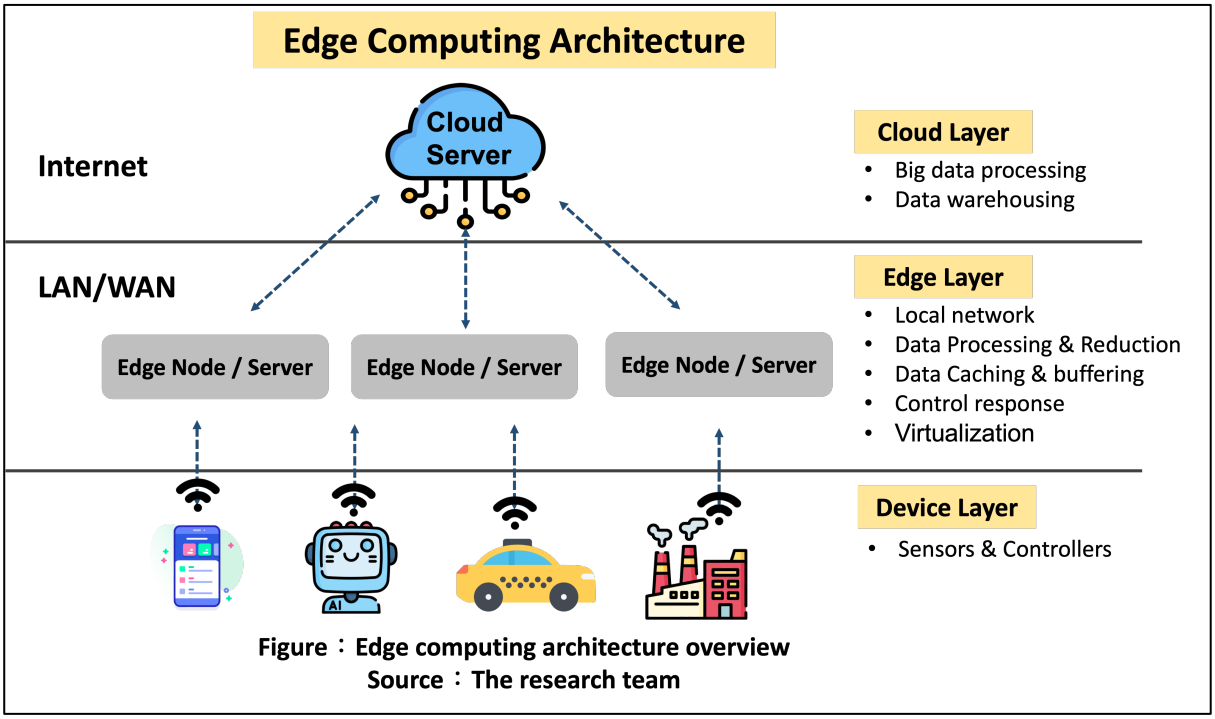

Figure 3. Edge-Cloud Computing Architecture (Augmented AI, 2023).

b. Localized Security Control

In addition to latency management, edge-cloud computing allows for more localized security measures. This means that data can be encrypted, processed, and analyzed closer to where it's generated, such as IoT devices or local servers (Zeyu et al., 2020; Nayyar et al., 2021). These measures lower interception risks and enhance cloud security by minimizing breach impacts before data reaches the cloud. Moreover, localized processing enables the execution of security protocols tailored to the specific data being handled in organizations. For instance, sensitive data can be processed on-

 doi:10.20944/preprints202501.0395.v1

premises to ensure that it never leaves a controlled environment, which is particularly important for cloud-reliant sectors like finance, where security is critical.

c. AI-Driven Threat Detection at the Edge

To further enhance security, Artificial Intelligence (AI) and Machine Learning (ML) can be integrated into edge devices. This integration allows for real-time threat detection and prevention (Huč, Šalej, and Trebar, 2021; Shah et al., 2022). These technologies analyze data patterns, learning from historical data to predict and identify anomalies. For instance, anomalies in data flow can be identified faster and addressed immediately at the edge to prevent them from reaching the cloud. Furthermore, these intelligent systems can automate responses to threats, such as separating compromised devices or blocking suspicious traffic, thereby minimizing the potential damage from security incidents.

d. Hybrid and Multi-Cloud Solutions

A hybrid cloud combines private (on-premises) and public cloud environments, while the use of multiple cloud services from different providers is referred to as multi-cloud (AlTwaijiry, 2021). A hybrid multi-cloud architecture, as shown in Figure 4, integrates both hybrid and multi-cloud setups. This strategy allows organizations to host their software in-house, migrate to a cloud provider as needed, and maintain the option to switch providers in the future.

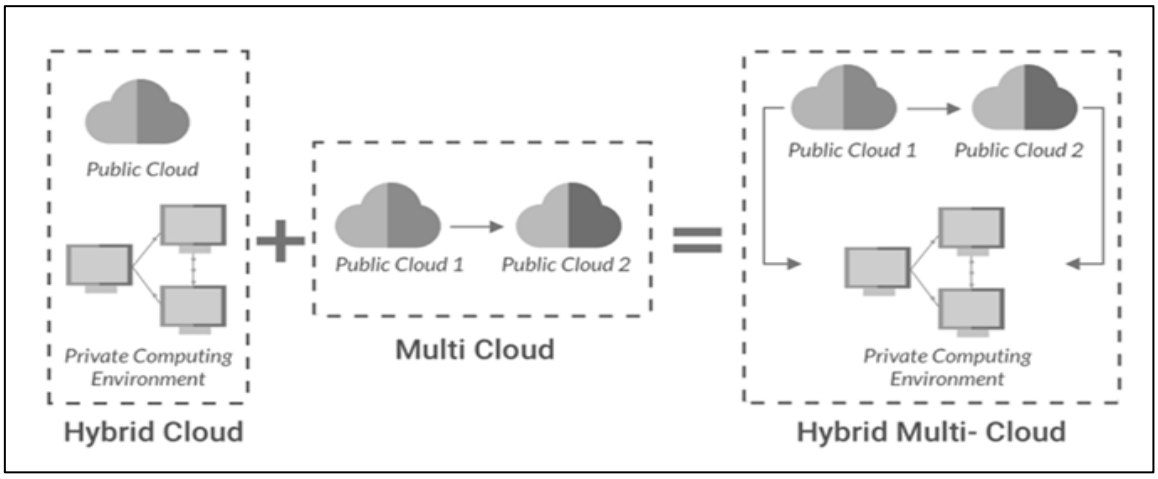

Figure 4. Hybrid Cloud and Multi-Cloud Architecture.

iv. Resilience Through Hybrid and Multi-Cloud Strategies

Hybrid and multi-cloud strategies help to enhance resilience by reducing reliance on a single cloud provider and distributing workloads across different platforms (McAuley, 2023; Sharma et al., 2021). If there is a security breach or outage with one cloud provider, the organization can continue operations with another provider, which helps reduce downtime and exposure. To support this resilience, secure communication across on-premises data centres, private clouds, and public clouds is essential for these multi-cloud strategies. This often requires advanced Virtual Private Network (VPN) solutions, secure APIs, and cloud security gateways to protect the data flows between the different cloud environments to ensure that data remains safe and accessible.

v. Zero-Trust Security for Hybrid Multi-Cloud Environments

To further secure hybrid and multi-cloud architectures, a zero-trust security model can be invaluable. This model assumes that all users and devices are untrusted until they can be properly authenticated (Papakonstantinou, 2021; Singhal et al., 2020). This approach helps minimize the risks associated with insider threats and unauthorized access to the systems and data of an organization.

 doi:10.20944/preprints202501.0395.v1

By limiting the impact of compromised credentials and blocking unauthorized lateral movement within cloud environments, zero-trust security strengthens an organization's defences. Using zero-trust tools and cloud-native security solutions can simplify security management, address the challenges of maintaining consistent security controls across platforms, and strengthen overall security posture. Proactively implementing these measures is crucial for organizations operating in complex multi-cloud environments. This proactive approach ensures that an organization's data and applications remain secure and accessible, even as the IT landscape becomes increasingly distributed and dynamic. (Alonso et al., 2023).

4. Discussion on Security Countermeasures

i. Security Countermeasures

a. Intrusion Detection System

Analyses the traffic activities and network traffic patterns to scan for any anomalies. Systems such as intrusion detection and prevention systems are a must-have for any cloud-related environment, for the Virtual Machine instance level and the network level. The Intrusion Detection System for the network will be able to detect the authentication or authorisation intrusions that open up vulnerabilities such as back door attacks, session hijacking etcetera. There are various types of IDS, for instance, Network-based IDS, Hypervisor-based IDS, Distributed IDS and Host-based IDS. (Google Cloud, 2024)

b. Digital Signature and Message Digest

Fundamental for data protection. A plethora of techniques may be used such as Symmetric encryption (AES), and Asymmetric encryption (RSA); these are widely adopted to try and prevent unauthorised access during data transmission and to secure data storage as a whole. Some companies use a hybrid cryptographic algorithm, which combines both symmetric and asymmetric encryption; it has proven effective in protecting the data whilst not compromising performance. More advanced encryption techniques like homomorphic encryption and attribute-based encryption (ABE) have also been tested to further improve the confidentiality of data. (Adobe help centre, 2023)

c. Comprehensive Security Measures

Cloud environments demand robust security mechanisms to safeguard resources, systems, and data. An approach which is multi-layered incorporating Identity and Access Management (IAM), network security, web application security, and data storage protection ensures comprehensive defence.

- Identity and Access Management (IAM): IAM serves as a core defence mechanism by controlling who accesses what resources. It employs strong authentication and authorization processes to verify users. Advanced authentication standards like OpenID Connect, Security Assertion Markup Language (SAML), and OAuth facilitate Multi-Factor Authentication (MFA), enhancing security. (Salama , S. *et al.* 2023)
- Network Security Measures: Measures such as Distributed Denial of Service (DDoS) protection, firewalls and Virtual Private Networks secure data communication. Firewalls control traffic based on security rules that are predefined, while VPNs encrypt data during transmission, mitigating interception risks. DDoS protection filters malicious traffic, ensuring availability during large-scale attacks. (Ometov, A. *et al.* 2022)
- Web Application Security: Web applications, central to most cloud environments, require rigorous countermeasures to address vulnerabilities. Security measures include digital signatures and XML encryption to ensure their integrity.

 doi:10.20944/preprints202501.0395.v1

- Data Storage Security: Data backups and disaster recovery plans safeguard the integrity and availability of data during system failures or cyberattacks. These strategies involve data replication, geo-redundancy, and redundant storage systems, ensuring data restoration with minimal downtime and losses. (Salama , S. *et al.* 2023)

ii. Proposed Countermeasures (Defense Solutions)

a. Intelligent Deception Technologies (Honeytokens and Honeynets)

Intelligent deception technologies like honeytokens and honeynets create fake data, systems, or resources specifically designed to attract and distract attackers. Unlike traditional detection systems, which react to suspicious activity passively, intelligent deception is a proactive approach that entices malicious users to interact with these decoy assets. This enables early detection of attackers' techniques, providing insights into their tactics, tools, and procedures (TTPs) without risking genuine data or systems. (Fortinet, 2023)

- **Honeytokens**: Fake data like fabricated database records, credentials, or document files, scattered throughout the cloud environment. A honeytoken could be a false set of keys embedded in a database. When attackers attempt to use or access these keys an alert is triggered, identifying and flagging suspicious activity early.
- **Honeynets**: Honeynets are networks of virtualized systems designed to simulate a real IT environment but hold no genuine data. When attackers infiltrate these decoys, they encounter a fully functional but isolated network that mimics legitimate cloud resources, capturing information on their methods without compromising real assets.

b. Innovation and Unique Features

1. **Machine Learning-Driven Deception**: ML algorithms analyze previous attack behaviours and intelligently place honeytokens or honeynets based on high-risk zones, such as user access points or areas with frequent external connections. Over time, the system learns to optimize token placement, adjust to emerging threats, and better adapt to specific cloud environments.
2. **Real-Time Threat Intelligence Collection**: When attackers interact with the decoys, the system logs their behaviours in detail, offering valuable data that can enhance threat intelligence. This insight helps organizations refine their security posture by understanding TTPs that attackers use to target cloud systems.
3. **Minimal Impact on System Performance**: Since honeytokens and honeynets do not hold real data, there's minimal risk to production systems, allowing organizations to adopt a more aggressive detection strategy without affecting legitimate workflows.

c. Technologies Used

a. **Machine Learning and AI**: ML algorithms are central to optimising honeytoken and honeynet deployment by analysing patterns of suspicious activity and identifying high-risk zones. AI-driven behavioural analytics can adapt the placement and characteristics of deception assets, making them harder for attackers to distinguish from real resources.

b. **Data Masking and Tokenization**: To make honeytokens more realistic, data masking and tokenization techniques can blur the actual data while creating convincing decoy records. This ensures that honeytokens mimic genuine data points.

 doi:10.20944/preprints202501.0395.v1

c. **Sandboxing and Virtualization**: Honeynets utilize virtualization and sandboxing to safely isolate decoy environments. This creates a controlled environment where attackers can be monitored and studied without risking actual production systems. These technologies enable honeynets to simulate various IT assets, including user endpoints, databases, and network nodes.

d. **Threat Intelligence Integration**: Integration with threat intelligence feeds and databases help update honeytokens and honeynets with the latest TTPs observed in real-world attacks. This allows the deception system to remain relevant and convincing as attackers' methods evolve.

d. How It's Innovative

- **Active Attacker Engagement**: Unlike traditional defences, which are primarily passive, intelligent deception engages and diverts attackers from real assets, extending the defensive perimeter.
- **Adaptation to Cloud Dynamics**: Deception technologies leverage ML to adapt dynamically within scalable cloud environments, keeping up with evolving configurations, user patterns, and emerging attack vectors.
- **Self-Learning and Optimization**: Machine learning allows these systems to improve continuously by learning from prior attack attempts, making decoys more realistic and placement more precise over time. (Javadpour, A. *et al.* 2024)

d. Evolution of Honeypot Technologies

Dynamic and Adaptive Deployment

- **Traditional Honeypots**: Typically static and require manual setup and tuning. They often remain in fixed locations within a network, making them easier for experienced attackers to detect and bypass over time.
- **Intelligent Deception**: Uses machine learning (ML) to dynamically place honeytokens and honeynets based on risk analysis. ML-driven insights allow these decoys to adapt by relocating or changing in response to evolving threats, increasing resilience against attacker evasion tactics. (Javadpour, A. *et al.* 2024)

e. Contextual Realism with Behavioral Analysis

- **Traditional Honeypots**: Often operate as isolated systems that may lack contextual relevance to the actual production environment, limiting their ability to blend in convincingly.
- **Intelligent Deception**: Leverages behavioural analysis to tailor honeytokens and honeynets to match typical user behaviours and legitimate data patterns, making decoys highly realistic and difficult to distinguish from real assets. This contextual accuracy makes these decoys more effective in luring attackers. (SentinelOne, 2024)

 doi:10.20944/preprints202501.0395.v1

f. AI-Driven Threat Prediction and Self-Learning

- **Traditional Honeypots**: Mostly reactive, capturing attacker activity after the attacker has entered the honeypot. They do not adapt based on attack patterns or improve their ability to attract attackers.
- **Intelligent Deception**: Incorporates AI-driven predictive analytics that can anticipate potential threats and adjust decoy placement to target high-risk areas. Self-learning capabilities mean these systems evolve continuously, optimizing their defences and maintaining relevance even as attacker methods change. (SentinelOne, 2024)

g. Integration with Threat Intelligence and Incident Response

- **Traditional Honeypots**: Typically lack integration with broader security frameworks, limiting their value to isolated threat detection.
- **Intelligent Deception**: Can integrate with threat intelligence feeds to reflect the latest TTPs (tactics, techniques, and procedures) used by attackers. Additionally, these systems often feed directly into incident response workflows, enabling automated responses like isolating affected areas, logging detailed activity, or deploying additional defences based on detected threats.(Javadpour, A. *et al.* 2024)

h. Reduced False Positives and Higher Alert Accuracy

- **Traditional Honeypots**: Might generate alerts whenever any interaction occurs, sometimes producing false positives that security teams must spend resources investigating.
- **Intelligent Deception**: Only triggers alerts upon genuine, malicious interactions with honeytokens or honeynets, reducing false positives and enhancing alert accuracy. This targeted approach enables security teams to focus on verified threats rather than dealing with benign or irrelevant alerts. (Javadpour, A. *et al.* 2024)

5. Conclusions

In conclusion, the cloud security report highlights the importance of implementing effective security approaches to protect sensitive data and infrastructure in cloud environments. While cloud security provides benefits like scalability, cost-effectiveness, and layered protection, it also brings challenges such as limited data control, regulatory issues, and multi-tenancy risks.

The report also points out the increasing threat of cyberattacks targeting cloud systems, including data breaches, malware, ransomware, and account hijacking. In order to minimise these risks, organizations need to implement comprehensive security strategies, such as intrusion detection systems, encryption techniques, and proactive solutions like honeytokens and honeynets.

As cyber threats become increasingly sophisticated, integrating artificial intelligence (AI) and machine learning (ML) technology into cloud security is becoming more vital. AI-driven solutions, like Google's Cloud Intrusion Detection System, improve threat detection by identifying intrusions, malware, and command-and-control attacks on networks (Google Cloud, 2024). Also, Microsoft's new data centre infrastructure chips are enhancing data processing speeds and security, highlighting the growing importance of AI in strengthening cloud security measures (Cherney, 2024). These

 doi:10.20944/preprints202501.0395.v1

technologies enable real-time detection, predictive analytics, and automated responses, improving overall security.

In the future, cloud security will likely depend more on adopting advanced solutions like edge-cloud and hybrid-cloud models to reduce latency and facilitate localized data processing. Additionally, the integration of artificial intelligence and machine learning into security strategies will be crucial for addressing emerging threats and guaranteeing the integrity and confidentiality of cloud data.

To sum up, maintaining robust cloud security requires organizations to stay adaptable to evolving cyber threats, prioritize the implementation of strong security frameworks, keep up with regulatory changes, and invest in cutting-edge technologies like AI and ML to protect their cloud infrastructures.

References

1. aditya191251015002 *et al.* (2024) *Architecture of Identity Access Management in cloud computing*, *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/architecture-of-identity-access-management-in-cloud-computing/.
2. Alex, S. A., Jhanjhi, N., Humayun, M., Ibrahim, A. O., & Abulfaraj, A. W. (2022). Deep LSTM Model for Diabetes Prediction with Class Balancing by SMOTE. *Electronics*, *11*(17), 2737. https://doi.org/10.3390/electronics11172737
3. Alferidah, D. K., & Jhanjhi, N. (2020). Cybersecurity Impact over Bigdata and IoT Growth. *2020 International Conference on Computational Intelligence (ICCI)*. https://doi.org/10.1109/icci51257.2020.9247722
4. Alkinani, M. H., Almazroi, A. A., Jhanjhi, N., & Khan, N. A. (2021). 5G and IoT Based Reporting and Accident Detection (RAD) System to Deliver First Aid Box Using Unmanned Aerial Vehicle. *Sensors*, *21*(20), 6905. https://doi.org/10.3390/s21206905
5. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., and Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, 9, pp.57792-57807. doi:https://doi.org/10.1109/ACCESS.2021.9404177.
6. AlTwaijiry, A. (2021). Cloud Computing Present Limitations and Future Trends. *ScienceOpen Preprints*. doi:https://doi.org/10.14293/s2199-1006.1.sor-.ppeyyii.v1.
7. Amos, K., Esquivel, R. and Esquivel, J.A. (2022). RANSOMWARE: RANSOMWARE AS A SERVICE (RaaS), METHODS TO DETECT, PREVENT, MITIGATE AND FUTURE DIRECTION. Available at: https://www.researchgate.net/publication/365349176_RANSOMWARE_RANSOMWARE_AS_A_SERVICE_RaaS_METHODS_TO_DETECTS_PREVENT_MITIGATE_AND_FUTURE_DIRECTION [Accessed 1 Nov. 2023].
8. Ananna, F. F., Nowreen, R., Jahwari, S. S. R. A., Costa, E. A., Angeline, L., & Sindiramutty, S. R. (2023). Analysing Influential factors in student academic achievement: Prediction modelling and insight. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.254
9. Arjun, R.K. (2023). Security Concerns and Solutions for Enterprise Cloud Computing Applications. *Asian Journal of Research in Computer Science*, 15(4), pp.24–33. doi:https://doi.org/10.9734/ajrcos/2023/v15i4327 [Accessed 3 Nov. 2024].
10. Augmented AI. (2023, March). *Will edge computing replace cloud computing? A comprehensive analysis*. https://www.augmentedstartups.com/blog/will-edge-computing-replace-cloud-computing-a-comprehensive-analysis
11. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.255
12. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., Tajwar, M. A., & Sindiramutty, S. R. (2023). Defending the digital Frontier: IDPS and the battle against Cyber threat. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.253

 doi:10.20944/preprints202501.0395.v1

13. Azam, H., Tajwar, M. A., Mayhialagan, S., Davis, A. J., Yik, C. J., Ali, D., & Sindiramutty, S. R. (2023). Innovations in Security: A study of cloud Computing and IoT. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.252
14. Azam, H., Tan, M., Pin, L. T., Syahmi, M. A., Qian, A. L. W., Jingyan, H., Uddin, M. F., & Sindiramutty, S. R. (2023). Wireless Technology Security and Privacy: A Comprehensive Study. *Preprints.org*. https://doi.org/10.20944/preprints202311.0664.v1
15. Babbar, H., Rani, S., Masud, M., Verma, S., Anand, D., & Jhanjhi, N. (2021). Load balancing algorithm for migrating switches in software-defined vehicular networks. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *67*(1), 1301–1316. https://doi.org/10.32604/cmc.2021.014627
16. Beerman, J., Berent, D., Falter, Z., and Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. Available at: https://sbhunia.me/publications/manuscripts/ccgrid23.pdf [Accessed 1 Nov. 2024].
17. Blessing, M. (2024). Cloud Encryption Strategies and Key Management. [pdf] p.10. Available at: https://www.researchgate.net/profile/Moses-Blessing/publication/383660212_Cloud_Encryption_Strategies_and_Key_Management/links/66d5b688fa5e11512c47d0eb/Cloud-Encryption-Strategies-and-Key-Management.pdf [Accessed 10 Nov. 2024].
18. Brohi, S. N., Jhanjhi, N., Brohi, N. N., & Brohi, M. N. (2020). Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19.pdf. *TECHRxiv*. https://doi.org/10.36227/techrxiv.12115596.v1
19. Brown, E. (2024). Advanced Techniques for Data Loss Prevention and Access Control in Big Data Cloud Infrastructures. *Advances in Computer Sciences*, [online] 7(1). Available at: https://academicpinnacle.com/index.php/acs/article/view/323 [Accessed 13 Nov. 2024].
20. Butt, U.A., Mehmood, M., Shah, S.B.H., Amin, R., Shaukat, M.W., Raza, S.M., Suh, D.Y., and Piran, M.J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, 9(9), p.1379. doi:https://doi.org/10.3390/electronics9091379.
21. Chauhan, M. and Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network, [online] 3(3), pp.422–450. doi:https://doi.org/10.3390/network3030018.
22. Chebitko, R. (2024, February 13). *What is a firewall and why is it used*. Softwareg.com.au. https://softwareg.com.au/blogs/internet-security/what-is-a-firewall-and-why-is-it-used
23. Cherney, M.A. (2024). Microsoft launches two data center infrastructure chips to speed up AI applications. Reuters.19 Nov. Available at: https://www.reuters.com/technology/artificial-intelligence/microsoft-launches-two-data-center-infrastructure-chips-speed-ai-applications-2024-11-19/.
24. Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. (2020). Evolution, Mitigation, and Prevention of Ransomware. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. https://doi.org/10.1109/iccis49240.2020.9257708
25. *Cloud IDS overview | Google Cloud* (2024) *Google*. Available at: https://cloud.google.com/intrusion-detection-system/docs/overview#:~:text=Cloud%20IDS%20is%20an%20intrusion,virtual%20machine%20(VM)%20instances
26. *Cloud-based digital signatures* (2023) *Adobe Help Center*. Available at: https://helpx.adobe.com/sign/config/send-settings/auth-methods/cloud-signature.html (Accessed: 1 November 2024).
27. Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M. and Rehman, S.U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*, [online] 15(11), pp.1–33. doi:https://doi.org/10.3390/sym15111981.
28. *Digital signatures | cloud KMS documentation | google cloud* (2024) *Google*. Available at: https://cloud.google.com/kms/docs/digital-signatures#:~:text=Digital%20signatures%20rely%20on%20asymmetric,used%20to%20verify%20the%20signature (Accessed: 1 November 2024).
29. Dogra, V., Singh, A., Verma, S., Kavita, N., Jhanjhi, N. Z., & Talib, M. N. (2021). Analyzing DistilBERT for Sentiment Classification of Banking Financial News. In *Lecture notes in networks and systems* (pp. 501–510). https://doi.org/10.1007/978-981-16-3153-5_53

 doi:10.20944/preprints202501.0395.v1

30. Dutta, S. (2024, March). *What are The Implications of Data Encryption for MIS?* Re School.
31. EDPB (2023). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. Available at: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en [Accessed 1 Nov. 2024].
32. El Kafhali, S., El Mir, I., and Hanini, M. (2021). Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering*, 29(1). doi:https://doi.org/10.1007/s11831-021-09573-y.
33. Fatima-Tuz-Zahra, N., Jhanjhi, N., Brohi, S. N., Malik, N. A., & Humayun, M. (2020). Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. https://doi.org/10.1109/iccis49240.2020.9257607
34. Garg, T., Saini, N., Singh, M., and Singh, S. (2024). Comparative Study of Security Threats in Cloud Computing. Available at: https://www.researchgate.net/publication/381193283_Comparative_Study_of_Security_Threats_in_Cloud_Computing [Accessed 1 Nov. 2024].
35. geeksforgeeks (2021). Security Issues in Cloud Computing. *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/security-issues-in-cloud-computing/.
36. Google Cloud, n.d. *What is cloud security?*. Available at: https://cloud.google.com/learn/what-is-cloud-security
37. Google Cloud. (2024). Cloud IDS overview. Available at: https://cloud.google.com/intrusion-detection-system/docs/overview?.
38. Gopi, R., Sathiyamoorthi, V., Selvakumar, S., Manikandan, R., Chatterjee, P., Jhanjhi, N. Z., & Luhach, A. K. (2021). Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimedia Tools and Applications*, *81*(19), 26739–26757. https://doi.org/10.1007/s11042-021-10640-6
39. Gouda, W., Almurafeh, M., Humayun, M., & Jhanjhi, N. Z. (2022). Detection of COVID-19 based on chest x-rays using deep learning. *Healthcare*, *10*(2), 343. https://doi.org/10.3390/healthcare10020343
40. Gurulcu (2023). Famous Insider Threat Cases. Available at: https://gurucul.com/blog/famous-insider-threat-cases [Accessed 1 Nov. 2024].
41. Hashim, W. and Noor (2024). Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures. [online] 2024, pp.9–17. doi:https://doi.org/10.70470/shifra/2024/002.
42. *Honey tokens: What are they and how are they used? Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/honey-tokens
43. Huč, A., Šalej, J., and Trebar, M. (2021). Analysis of Machine Learning Algorithms for Anomaly Detection on Edge Devices. *Sensors*, 21(14), p.4946. doi:https://doi.org/10.3390/s21144946.
44. Humayun, M., Sujatha, R., Almuayqil, S. N., & Jhanjhi, N. Z. (2022). A Transfer Learning Approach with a Convolutional Neural Network for the Classification of Lung Carcinoma. *Healthcare*, *10*(6), 1058. https://doi.org/10.3390/healthcare10061058
45. Hussain, K., Rahmatyar, A. R., Riskhan, B., Sheikh, M. a. U., & Sindiramutty, S. R. (2024). Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT). *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, *2*, 1–8. https://doi.org/10.1109/khi-htc60760.2024.10482197
46. IAIC (2020). *IAIC Transactions on Sustainable Digital Innovation (ITSDI) The 2nd Edition Vol. 1 No. 2 April 2020*. Available at: https://books.google.com.my/books?id=VccwEAAAQBAJ.
47. IBM, 2024. *Cloud security*. Available at: https://www.ibm.com/topics/cloud-security
48. IBM, 2024. *Cost of a data breach 2024*. Available at: https://www.ibm.com/reports/data-breach
49. Jack, B., David, B., Zach, F., and Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. Available at: https://sbhunia.me/publications/manuscripts/ccgrid23.pdf [Accessed 1 Nov. 2024].
50. Javadpour, A. *et al.* (2024) *A comprehensive survey on cyber deception techniques to improve honeypot performance*, *Computers & Security*. Available at: https://www.sciencedirect.com/science/article/pii/S0167404824000932(Accessed: 13 November 2024).
51. Jhanjhi, N., Humayun, M., & Almuayqil, S. N. (2021). Cyber security and privacy issues in industrial internet of things. *Computer Systems Science and Engineering*, *37*(3), 361–380. https://doi.org/10.32604/csse.2021.015206

52. Jun, A. Y. M., Jinu, B. A., Seng, L. K., Maharaiq, M. H. F. B. Z., Khongsuwan, W., Junn, B. T. K., Hao, A. a. W., & Sindiramutty, S. R. (2024). Exploring the Impact of Crypto-Ransomware on Critical Industries: Case Studies and Solutions. *Preprints.org*. https://doi.org/10.20944/preprints202409.1325.v1
53. Kaspersky, 2020. *What is cloud security?*. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security
54. Krebs, B. (2023). New T-Mobile Breach Affects 37 Million Accounts. Available at: https://krebsonsecurity.com/2023/01/new-t-mobile-breach-affects-37-million-accounts
55. Kumar, M. S., Vimal, S., Jhanjhi, N., Dhanabalan, S. S., & Alhumyani, H. A. (2021). Blockchain based peer to peer communication in autonomous drone operation. *Energy Reports*, *7*, 7925–7939. https://doi.org/10.1016/j.egyr.2021.08.073
56. Kumar, S., Rajlingam, A., Gokila, B., and Arunkumar, J. (2023). Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies. *Journal of Science, Computing and Engineering Research*, 6(6), pp.6–10. doi:https://doi.org/10.46379/jscer.2023.0608002.
57. Kunduru, A.R. (2023). THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW. *CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES*, [online] 4(9), pp.29–41. Available at: https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/515.
58. Lata, S. and Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. *International Journal of Information Management Data Insights*, [online] 2(2), p.100134. doi:https://doi.org/10.1016/j.jjimei.2022.100134.
59. Lim, M., Abdullah, A., Jhanjhi, N., Khan, M. K., & Supramaniam, M. (2019). Link Prediction in Time-Evolving Criminal Network with deep Reinforcement learning technique. *IEEE Access*, *7*, 184797–184807. https://doi.org/10.1109/access.2019.2958873
60. Manchuri, A., Kakera, A., Saleh, A., & Raja, S. (2024). pplication of Supervised Machine Learning Models in Biodiesel Production Research - A Short Review. *Borneo Journal of Sciences and Technology*. https://doi.org/10.35370/bjost.2024.6.1-10
61. McAuley, D. (2023). Hybrid and Multi-Cloud Strategies: Balancing Flexibility and Complexity. *MZ Computing Journal*, 4(2). Available at: https://mzjournal.com/index.php/MZCJ/article/view/313
62. Nayyar, A., Gadhavi, L., & Zaman, N. (2021). Machine learning in healthcare: review, opportunities and challenges. In *Elsevier eBooks* (pp. 23–45). https://doi.org/10.1016/b978-0-12-821229-5.00011-2
63. Ometov, A. *et al.* (2022) *A Survey of Security in Cloud, Edge, and Fog Computing*, *https://www.mdpi.com/journal/sensors*. Available at: chrome-extension://gphandlahdpffmccakmbngmbjnjiiahp/https://mdpi-res.com/d_attachment/sensors/sensors-22-00927/article_deploy/sensors-22-00927.pdf?version=1643114960(Accessed: 01 November 2024).
64. Papakonstantinou, N., Van Bossuyt, D.L., Linnosmaa, J., Hale, B. and O'Halloran, B. (2021). A Zero Trust Hybrid Security and Safety Risk Analysis Method. *Journal of Computing and Information Science in Engineering*, pp.1–26. doi:https://doi.org/10.1115/1.4050685.
65. PECB (2023). Cloud Computing Security: Top Challenges and How to Mitigate Them. Available at: https://pecb.com/article/cloud-computing-security-top-challenges-and-how-to-mitigate-them.
66. Practical Cloud Security A Guide for Secure Design and Deployment. (n.d.). Available at: https://orca.security/wp-content/uploads/2021/12/pracCloudSecurity.pdf.
67. Rashid, A. and Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, 7(2), pp.421-426. Available at: https://www.researchgate.net/publication/331731714_Cloud_Computing_Characteristics_and_Services_A_Brief_Review.
68. Ravichandran, N., Tewaraja, T., Rajasegaran, V., Kumar, S. S., Gunasekar, S. K. L., & Sindiramutty, S. R. (2024). Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks. *Preprints.org*. https://doi.org/10.20944/preprints202409.1369.v1
69. Salama , S. *et al.* (2023) *Cloud Computing Security Issues and Countermeasure: A Comprehensive Survey*, *International Journal of Computer Applications*. Available at: chrome-extension://gphandlahdpffmccakmbngmbjnjiiahp/https://cdn.discordapp.com/attachments/110795275732

 doi:10.20944/preprints202501.0395.v1

0724611/1299234999249145866/salama-2023-ijca-922832.pdf?ex=673ac8e2&is=67397762&hm=be585808b85d92b7e2992f881c6c120afc7ab2565cd2f40e15dcfa0e69dcac3f&(Accessed: 28 October 2024).

70. Schulze, H. (2023). 2023 Insider Threat Report. Available at: https://www.cybersecurity-insiders.com/wp-content/uploads/2023/01/2023_Insider_Threat_Report-16d8d8f7.pdf[Accessed 1 Nov. 2024].
71. Seng, Y. J., Cen, T. Y., Raslan, M. a. H. B. M., Subramaniam, M. R., Xin, L. Y., Kin, S. J., Long, M. S., & Sindiramutty, S. R. (2024). In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations. *Preprints.org*. https://doi.org/10.20944/preprints202408.2261.v1
72. Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2022). Cybersecurity and blockchain usage in contemporary business. In *Advances in information security, privacy, and ethics book series* (pp. 49–64). https://doi.org/10.4018/978-1-6684-5284-4.ch003
73. Sharma, R., Singh, A., Kavita, N., Jhanjhi, N. Z., Masud, M., Jaha, E. S., & Verma, S. (2021). Plant disease diagnosis and image classification using deep learning. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *71*(2), 2125–2140. https://doi.org/10.32604/cmc.2022.020017
74. Sheriffdeen, K. (2022). Integrating Cloud-Based Solutions in Disaster Recovery Planning. [pdf] p.20. Available at: https://www.researchgate.net/profile/Martins-Ade/publication/383849282_Integrating_Cloud-Based_Solutions_in_Disaster_Recovery_Planning/links/66dc87562390e50b2c729284/Integrating-Cloud-Based-Solutions-in-Disaster-Recovery-Planning.pdf [Accessed 14 Nov. 2024].
75. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., & Manchuri, A. R. (2024). Cybersecurity measures for logistics industry. In *Advances in information security, privacy, and ethics book series* (pp. 1–58). https://doi.org/10.4018/979-8-3693-3816-2.ch001
76. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., Yun, K. J., Ray, S. K., Jazri, H., & Hussain, M. (2024). Future trends and emerging threats in drone cybersecurity. In *Advances in information security, privacy, and ethics book series* (pp. 148–195). https://doi.org/10.4018/979-8-3693-0774-8.ch007
77. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Yun, K. J., Manchuri, A. R., Ashraf, H., Murugesan, R. K., Tee, W. J., & Hussain, M. (2024). Data security and privacy concerns in drone operations. In *Advances in information security, privacy, and ethics book series* (pp. 236–290). https://doi.org/10.4018/979-8-3693-0774-8.ch010
78. Sindiramutty, S. R., Jhanjhi, N., Tan, C. E., Lau, S. P., Muniandy, L., Gharib, A. H., Ashraf, H., & Murugesan, R. K. (2024). Industry 4.0. In *Advances in logistics, operations, and management science book series* (pp. 342–405). https://doi.org/10.4018/979-8-3693-1363-3.ch013
79. Sindiramutty, S. R., Tan, C. E., & Wei, G. W. (2024). Eyes in the sky. In *Advances in information security, privacy, and ethics book series* (pp. 405–451). https://doi.org/10.4018/979-8-3693-0774-8.ch017
80. Sindiramutty, S. R., Tan, C. E., Shah, B., Khan, N. A., Gharib, A. H., Manchuri, A. R., Muniandy, L., Ray, S. K., & Jazri, H. (2024). Ethical considerations in drone cybersecurity. In *Advances in information security, privacy, and ethics book series* (pp. 42–87). https://doi.org/10.4018/979-8-3693-0774-8.ch003
81. Singhal, V., Jain, S. S., Anand, D., Singh, A., Verma, S., Kavita, N., Rodrigues, J. J. P. C., Jhanjhi, N. Z., Ghosh, U., Jo, O., & Iwendi, C. (2020). Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned railway level crossings. *IEEE Access*, *8*, 113790–113806. https://doi.org/10.1109/access.2020.3002416
82. Tabrizchi, H. and Rafsanjani, M.K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, [online] 76(12), pp.9493–9532. doi:https://doi.org/10.1007/s11227-020-03213-1.
83. Technical Review. *Future Internet*, 14(1), p.11. doi:https://doi.org/10.3390/fi14010011.
84. Tisha, G., Neha, S., Manjeet, S., and Shalu, S. (2024). Comparative Study of Security Threats in Cloud Computing. Available at: https://www.researchgate.net/publication/381193283_Comparative_Study_of_Security_Threats_in_Cloud_Computing [Accessed 1 Nov. 2024].

85. Ul Haq, M.N. and Sharma, M.K. (2023). MASTERING CLOUD SECURITY: TECHNIQUES AND BEST PRACTICES. *EMERGING TRENDS IN CLOUD SECURITY AND INTELLIGENT AGENTS*. [online] doi:https://doi.org/10.52458/9788196869434.2023.eb.grf.ch-07.
86. Waheed, A., Seegolam, B., Jowaheer, M. F., Sze, C. L. X., Hua, E. T. F., & Sindiramutty, S. R. (2024). Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure. *preprints.org*. https://doi.org/10.20944/preprints202407.2338.v1
87. Wen, B. O. T., Syahriza, N., Xian, N. C. W., Wei, N. G., Shen, T. Z., Hin, Y. Z., Sindiramutty, S. R., & Nicole, T. Y. F. (2023). Detecting cyber threats with a Graph-Based NIDPS. In *Advances in logistics, operations, and management science book series* (pp. 36–74). https://doi.org/10.4018/978-1-6684-7625-3.ch002
88. *What is honeypot? working, types & benefits* (2024) *SentinelOne*. Available at: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/honeypot-cyber-security/(Accessed: 13 November 2024).
89. Zeyu, H., Geming, X., Zhaohang, W., and Sen, Y. (2020). Survey on Edge Computing Security. *IEEE Xplore*. doi:https://doi.org/10.1109/ICBAIE49996.2020.00027.