Towards a Secure Cloud Ecosystem: Innovations in Cybersecurity

Anamallah Bin Samshul Kamar , Au Cheng Hong Eddy , Brendan Wong Chun Bing , Chow Wen Jun , Dillon Teh Whei Teik , Lee Kah Fatt , Loh Wei Hao , Mohamed Jawad Haider Rajpar , Sean Ng Jun Zi , Yeo Hao Zen , Siva Raja Sindiramutty *

Posted Date: 7 January 2025

doi: 10.20944/preprints202501.0494.v1

Keywords: Cloud Computing Security; Identity and Access Management (IAM); Intrusion Detection Systems (IDS); Zero Trust Architecture; AI-Driven Threat Detection

Towards a Secure Cloud Ecosystem: Innovations in Cybersecurity

Anamallah Bin Samshul Kamar, Au Cheng Hong Eddy, Brendan Wong Chun Bing, Chow Wen Jun, Dillon Teh Whei Teik, Lee Kah Fatt, Loh Wei Hao, Mohamed Jawad Haider Rajpar, Sean Ng Jun Zi, Yeo Hao Zen and Siva Raja Sindiramutty *

0361232@sd.taylors.edu.my (A.B.S.K.); auchenghong.eddy@sd.taylors.edu.my (A.C.H.E.); 0362223@sd.taylors.edu.my (B.W.C.B.); chow.wenjun@sd.taylors.edu.my (C.W.J.); dillonwheiteik.teh@sd.taylors.edu.my (S.T.W.T.); kahfatt.lee@sd.taylors.edu.my (L.K.F.); 0363316@sd.taylors.edu.my (L.W.H.); 0365144@sd.taylors.edu.my (M.H.H.R.); 0369733@sd.taylors.edu.my (S.N.J.Z.); 0369886@sd.taylors.edu.my (Y.H.Z.)

* Correspondence: magan.shiva91@gmail.com

Abstract: Cloud computing has become a fundamental part of many households and organizations today offering many advantages such as cost savings, scalability, remote accessibility and more making it a foundational component of modern digital infrastructure. Along with the benefits of cloud computing, it also introduces significant security challenges that are the primary concern of many people and organisations as it contains the private data of many stakeholders. To address the vulnerabilities, security-related technologies such as encryption, firewalls, Intrusion Detection Systems (IDS), Identity and Access Management (IAM) and Service Level Agreements (SLA) should be considered. This paper aims to investigate the details of security-related technologies such as their components and processes to justify how the security-related technologies can help cloud-based systems combat their vulnerabilities ensuring the best interests of those involved. The paper consists of a background, detailed discussion on how security-related technology works, the impact and limitations of cloud computing, cloud computing's potential, security countermeasures and proposed countermeasures. Through the analysis of all the discussed topics, the paper aims to provide a comprehensive understanding of the importance of adopting security-related technologies in maintaining a secure and optimised cloud-based system.

Keywords: Cloud Computing Security; Identity and Access Management (IAM); Intrusion Detection Systems (IDS); Zero Trust Architecture; AI-Driven Threat Detection

1. Background

In today's era, cloud computing always controls the technology landscape. With over 90% of enterprises adopting cloud services, it can easily reveal how most companies manage their information technology resources. When it comes to the benefits, cloud computing possesses scalability, flexibility and most importantly, cost efficiency. These benefits make businesses innovate rapidly and change the market demands.

However, the changes in cloud-based infrastructure are causing significant security challenges that must be overcome so that sensitive data can be stored safely with a high level of security, and maintain organisational integrity. When it comes to the other challenge, it is misconfiguration. Many organisations may not set up their cloud services in the correct ways, causing vulnerabilities that will allow hackers to take advantage of them. So, examining regularly and updating the configurations is extremely important to prevent these serious issues.

Next, compliance with regulations is also part of the concern, which all organisations must obey laws such as the General Data Protection Regulation (GDPR) or Portability and Accountability Act (HIPAA), which require rigorous data protection measures. If organisations do not comply with these

 doi:10.20944/preprints202501.0494.v1

laws, organisations need to pay hefty fines which also results in the organisation's reputation. (Mission Cloud, 2024) Additionally, insider threats also pose a risk (Mission Cloud, 2024). For instance, employees who can access the company's sensitive data may intentionally or unintentionally compromise security. So, implementing measures such as strict access controls and monitoring user activity helps to mitigate the risk.

When it comes to convenience, cloud services are one of them, but it also comes with critical responsibilities, such as a shared responsibility model, splitting between cloud service providers (CSPs) and the organisations using the cloud to secure the application and data (Wiz, 2024). These factors create vulnerabilities that can be easily exploited by cybercriminals, causing data breaches, unauthorised access and compliance violations (CloudZero, 2024). According to CloudZero (2024), "cloud computing was already booming before 2020. But in the following years, remote work flourished, and cloud adoption soared." (CloudZero). The need for robust security measures becomes topmost.

To ensure data is safe in the cloud, it is important for organisations to utilise additional tools that are made for their cloud systems, such as encryption, identity, access management (IAM) and multi-factor authentication (2FA) which are helpful in making sure data is safe. These tools not only reduce the potential risks but also enhance the overall security readiness of organisations operating in the cloud.

2. Detailed Discussion on How Security-Related Technology Works

2.1. Component

2.1.1. Identity and Access Management (IAM)

Identity and Access Management, known as IAM, is a framework which ensures that the right individuals and entities have the appropriate access to cloud resources. At the same time, preventing unauthorized access to those who shouldn't have access. (Ahmadi, 2024; Ananna et al., 2023) With that said, IAM plays a crucial role in maintaining security and compliance using managing user identities, roles, access controls, and permissions which are within the cloud environment.

For IAM to work accordingly, it would contain the following key features:

User Identity Management: Centralizes the creation, management, and deletion of user accounts on the cloud environment. As well as supporting single sign-on capabilities which allows users to access multiple applications with only just one set of credentials. (Ej-eng.org, 2024)

Access Policies: Definition of access policies that specify which users can have access to which resources and under which conditions like time, and location. (Ieee.org, 2024; Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023) Authentication Methods: Authentication to ensure that the user is who they say they are by making them prove by passwords, biometrics, multi-factor authentication, and many others. (Ahmadi, 2024; Ieee.org, 2024) Audit: Tracks and keeps records of user activity and access patterns to maintain logs for audits. This can generate reports that can be used to help understand patterns and any other potential security threats. (Achar, 2022)

2.1.2. Encryption

Encryption plays a crucial role in cloud computing as it is used to protect sensitive data by converting the data to unreadable code. This would only allow authorized users to access the data using a decryption key. This is especially true in a cloud environment where data is moved from place to place such as data centers, network devices, and other parts of cloud environments. (Achar, 2022; Shukla, Dwivedi and Trivedi, 2020; Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023) By securing the data, encryption would help prevent data breaches, uphold privacy standards, and most importantly meet regulatory compliance requirements. Data Encryption at Rest/Transit: Encrypts data stored either on physical disk or in the cloud when data is being moved across networks, by securing the data from unauthorized access even when the data is hacked into. This is done by using symmetric or asymmetric keys, and Hypertext Transfer Protocol Secure and Transport Layer Security. (Sana et al., 2021)

 doi:10.20944/preprints202501.0494.v1

Asymmetric Encryption: Uses pairs of keys a public key for encryption and a private key for decryption. This is much more secure as the private key is generated and kept within each entity instead of transferred, which can lead to the key being leaked. (Hossein Abroshan, 2021)

2.1.3. Firewalls & Intrusion Detection Systems (IDS)

Firewalls and IDS are both important components where they lay down the fundamentals of a protective barrier between the cloud environment and any potential threats from entering. Firewalls would control the incoming and outgoing traffic based on the security policies enforced which would directly prevent unauthorized access. As for IDS, it works by detecting and alerting admins on potential malicious activities within the cloud environment. Both firewalls and IDS are crucial to ensure security from outside and possible inside threats. (Ariyanto et al., 2020) (Rana et al., 2022)

Firewalls key feature that defends the cloud environment include:

Traffic Control: Firewalls would filter through incoming and outgoing traffic based on the pre-established security policies. This would only allow authorized access to the cloud environment. The policy rules include IP addresses, port numbers, and many others. (Ariyanto et al., 2020)

As for Intrusion Detection Systems, the key features includes:

Network-Based IDS: NIDS monitors and analyzes network traffic for any signs of malicious activity. (Rana et al., 2022) Host-Based IDS: HIDS monitors pre-determined cloud resources, focusing on logs, system files, and configurations. (Rana et al., 2022; Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023) Signature-Based IDS: Signature-based IDS utilizes known threat patterns to detect attacks. This is very effective against common attacks; however, it proves to be not as effective against new and unknown threats. (E Balamurugan et al., 2022) Anomaly Based IDS: Anomaly Based IDS identifies unusual patterns or behaviors in the environment which increases its capabilities of detecting zero-days. (K. Samunnisa, Kumar and K. Madhavi, 2022; Al-Ghuwairi et al., 2023)

Log and Alert: IDS generates and sends alerts for any potential threats and suspicious activities. This would allow the admins to react and deal with the situation promptly. The logs generated can also be integrated with Security Information and Event Management tools for centralized monitoring, analysis, and incident response much more easily. (Achar, 2022; Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023)

2.1.4. Service Level Agreements (SLA)

SLAs is to provide a measurable framework for security requirements and accountability. By defining metrics, responsibilities, and accountability, SLA would be able to establish a security policy that could be followed to secure the cloud environment. Ensuring protection on the agreed-upon level of data security, uptime, and incident response. Additionally holding the cloud security service provider accountable for meeting the commitments. (Seid et al., 2024; Hussain et al., 2024).

For SLA to be effective, it would need to include key features such as:

Accountability & Transparency: With the SLA framework created, setting up clear expectations for the security and performance of the cloud environment, sets up accountability of the service provider. The service provider would then be obligated to meet the specified standards with transparency gained from the provider's practices. (Ismail and Islam, 2020; Jun et al., 2024).

Data Protection and Compliance: With that said, it is also very important to ensure the security policies are up to date and align with the industry standards which would enhance the security of the cloud environment. (None Zein Samira et al., 2024; Manchuri et al., 2024).

Regular Assessment/Audit: SLAs would perform regular assessments of the service provider's security practices through monitoring. This would enable any possible improvement of the security policies. (Ismail and Islam, 2020; Ravichandran et al., 2024).

 doi:10.20944/preprints202501.0494.v1

2.2. PROCESS

Identity and Access Management (IAM) Process

1. User Authentication: The first two phases of IAM are identification and authentication, which validate users based on either password, biometric analysis, or MFA authentication. When the user logs in and tries to access cloud resources, they must prove their identity through one of these techniques, thereby allowing the actual user to proceed.
2. Access Provisioning: IAM authenticates the users and provides them with roles and levels of access as defined by its policies for Role-Based Access Control. The ultimate goal of provisioning is to ensure users are provided with no more permissions than are necessary to perform their functions, to minimise exposure to sensitive data.
3. Continuous Monitoring: IAM always monitors the pattern of access by users and logs their activities. When it finds any anomaly, IAM may ask for re-authentication or even alert administrators to take appropriate action, hence introducing another layer of security.
4. Audit and Compliance: IAM provides compliance and audit log support for the traceability of user actions, which is important in threat detection.

2.2.1. Encryption Process

1. Key Generation and Storage: The encryption process begins with the generation of an exclusive encryption key. Most often, cloud service providers use Hardware Security Modules to provide secure key management and keep all keys confidential and temper evident.
2. Data Encryption:

Rest: Data at rest stored in the cloud is kept encrypted and access is granted to it only in a restricted manner.

In transit: When the data is in network transit, encryption protocols such as TLS encrypt it to make it secure from interceptions.

3. Data Encryption: Encrypted data is made accessible to an authorized user or application by decrypting it with the proper key.
4. Key Management and Rotation: Keys are changed out or renewed periodically to maintain security. Key management policies indicate the frequency of rotation and how keys are disposed of after use.

2.2.2. Firewalls and Intrusion Detection Systems (IDS) Process

1. Traffic Filtering (Firewall): Firewalls analyse the entrance and exit traffic against security policies. In case a request matches the rules of the firewall, then it is granted and in case of mismatch, it is rejected, thus preventing unauthorised access.
2. Segmentation and Access Control: Firewalls segment network areas which allow sensitive data to be kept in zones away from general access. In this regard, if there is a breach, it will be restricted to smaller areas.
3. Intrusion Detection (IDS): IDS carries out continuous monitoring of network traffic. Using signature-based and anomaly-based detection techniques, the suspect pattern of traffic is identified, and administrators are alerted for further cause to suspect security threats.
4. Incident Response: When an anomaly is detected, it logs the details and informs the security teams. Teams would then investigate and respond with speed and, when necessary, isolate parts of the network to limit the extent of the compromise.

2.2.3. Service Level Agreements (SLA) Enforcement Process

1. Defining Security Metrics: First, the SLAs establish quantifiable measures for standards, such as uptimes, data protection, or incident response times. Naturally, these standards would form the basis for a review of service performance.

 doi:10.20944/preprints202501.0494.v1

2. Ongoing Monitoring and Assessment: Providers of cloud services are continuously implementing security within their operations, assessing whether or not they are meeting their SLA standards. Common audits are performed to confirm practices with security commitments.
3. Incident Management and Reporting: In the case of a security incident, providers shall be responsible for acting if applicable, as specified in the time frames according to the SLA, reporting the details and corrective actions taken transparently to the clients.
4. Feedback and Change: SLAs can be revised periodically for new security requirements or enhancements to meet industry standards.

2.3. Threat

Cloud computing is one of the trendiest forms of technology due to its resources such as infrastructure, software and platform, which can be accessed and used virtually anywhere around the world (Gaur et al, 2023). Hence, making it cost-effective and scalable. When it comes to cloud computing, security plays a crucial role as 94% of enterprises have used cloud computing for their servers, applications and storage of data (Brown, 2024; Seng et al., 2024). This makes it vulnerable for attackers to conduct unauthorised access and other malicious activities. The most common 5 types of threats which cloud computing security can access and the approach or tools to stop them are as follows:

2.3.1. Misconfiguration

According to Brown (2024), it is often caused by misconfigured system setups or operations which can leave the systems vulnerable to all sorts of attacks since cloud computing is a very fine process. For instance, if the cloud was accidentally configured in such a way that any department within an organisation can access the entire network or database, dishonest workers may take advantage of it. Moreover, it is more of a risk rather than a threat as it involves human error and poor configuration planning.

The best way to deal with misconfiguration is by using cloud security posture management (CSPM). According to Microsoft (2024), CSPM helps to detect any configuration errors and improper settings, as well as ensuring it meets security standards and compliance policy. Other than that, it also has a monitoring and automation feature that corrects any mistakes without human error. Figure 1 shows an example of misconfiguration.

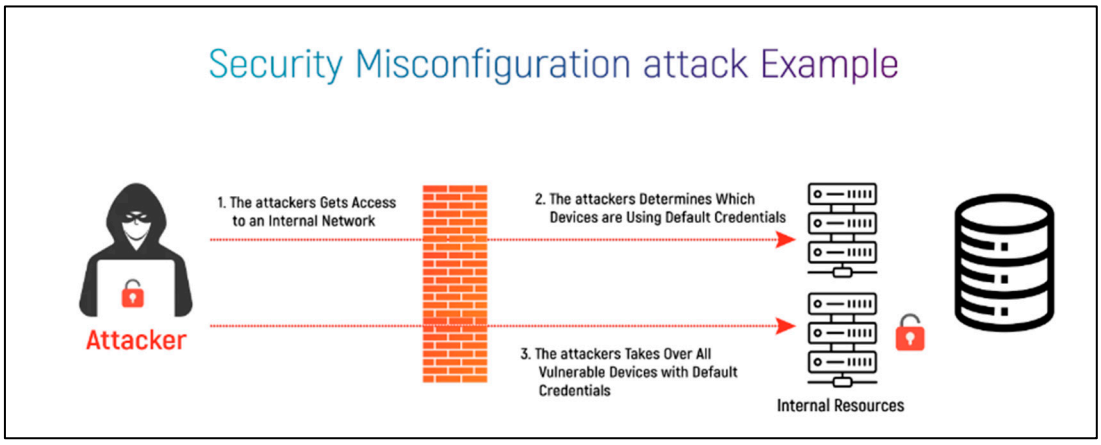

Figure 1. Example of misconfiguration (Rajeswari Baby Natchiar M, 2023).

2.3.2. Insider Threats

(Deemer, 2024) Inside threats are the misuse or improper handling of data, specifically by employees working in the organisation who have a lot of access to confidential information and might try to steal the data, damaging the company's reputation and image. Thus, resulting in financial loss.

 doi:10.20944/preprints202501.0494.v1

Sometimes, it may not even be intentional as employees might fall for malicious links or phishing scams where attackers will be able to access confidential data.

Access controls and education are some of the best approaches to reducing insider threats (Deemer, 2024; Sindiramutty et al., 2024). Access control enables certain users depending on their roles to access limited information or resources within the cloud, as well as multi-factor authentication. In addition, education helps to ensure that employees are aware of insider threats and how to properly manage sensitive data. Figure 2 show types and examples of Insider threats.

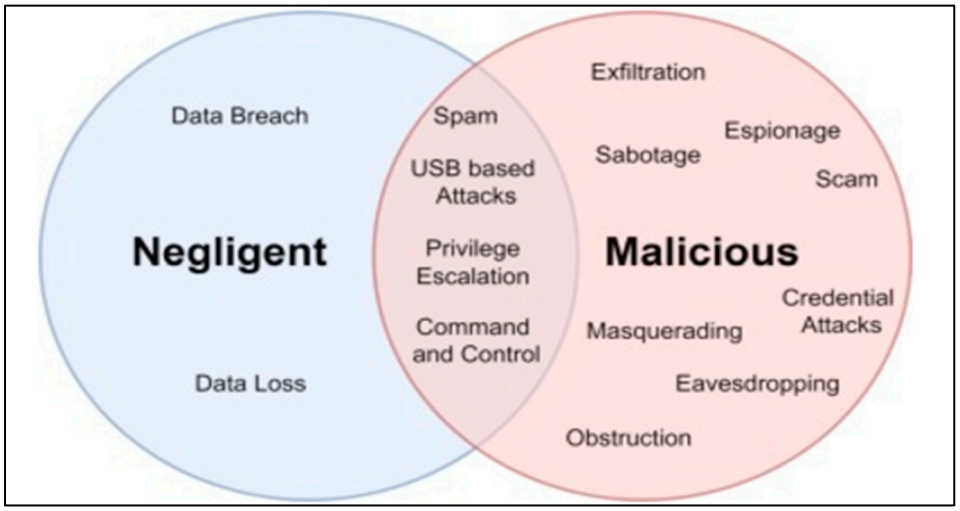

Figure 2. Types and examples of Insider threats. (Usman Inayat et al., 2024).

2.3.3. Data Loss

Deemer (2024) states that cloud computing, even though it is strong and resilient, is still prompt to data loss. It is usually caused by human error, specifically accidental deletion or corrupted data, but mostly due to ransomware attacks. Ransomware usually involves an attacker encrypting data to threaten an organisation in exchange for a large sum of money within a period to get the key for decryption. The worst case would be the attacker deleting the data and making it disastrous for the company to retrieve the lost information.

There are numerous ways to prevent data loss by Sajid (2023), but the simplest and most common are data backups and encryption. Data backups ensure that in the event of cyberattacks, it can be easily retrieved since all the copied data resources are stored elsewhere (Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024). While encryption does not necessarily guarantee data is inaccessible by attackers, it does make it unreadable without a decryption key. Hence, unauthorised personnel will not be able to take advantage of it.

2.3.4. Account Hijacking

This form of threat involves the attackers infiltrating a cloud user's account or resources through brute force attacks, phishing scams or other malicious ways. While doing so, they will act as legitimate users gain unauthorised access to sensitive information and disrupt the operations of the company. Figure 3 shows an example of account hijacking, The best approach for account hijacking is multi-factor authentication which adds a layer of security and strong passwords to make it harder to guess via brute force. Other than that, spreading awareness and properly educating your employees give them valuable insights into the danger of cyberattacks such as malware or phishing scams.

 doi:10.20944/preprints202501.0494.v1

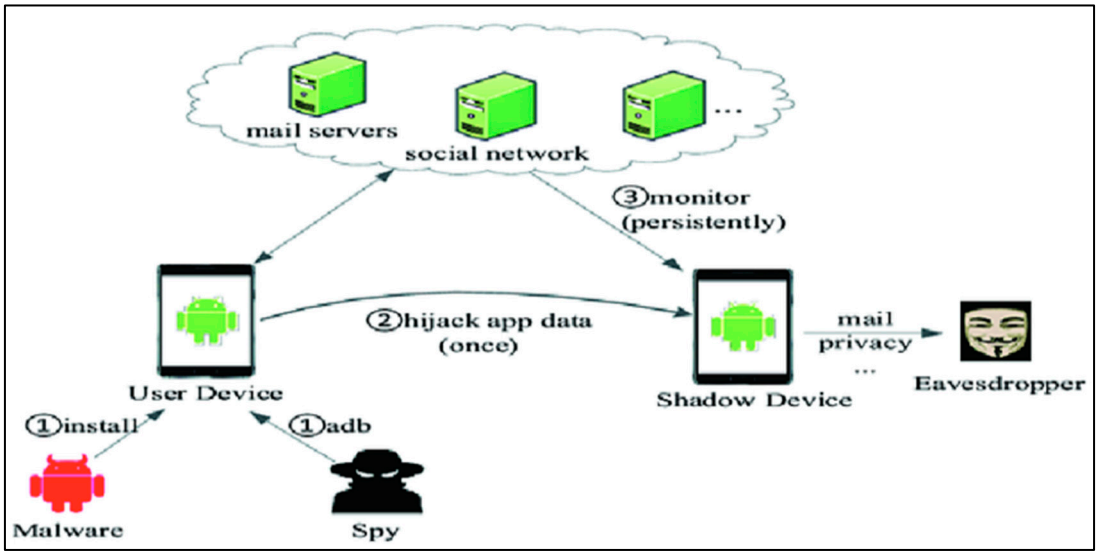

Figure 3. Example of Account Hijacking (Yadav, Kalaskar and Dhumane, 2023).

2.3.5. Denial of Service

Edwards (2024) mentions that it is a form of overwhelming cloud services or resources with traffic. Even though it does not cause data loss or breaches, it overloads the server's memory and degrades the performance (Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024). Hence, causing the flow of operations to be disrupted and delayed. In other words, businesses will have financial loss leading to a decline in business reputation.

Denial of Service can be easily managed by rate limiting and load balancing. Rate limiting works simply by limiting the number of requests within a time frame from a specific IP address and any request beyond the limit will not be met, as well as warning the users (HAProxy, 2024; Sindiramutty et al., 2024). Load balancing normally works by giving clients cooldown duration if they were detected of suspicious activity. Figure 4 shows denials of the service attack mechanism. Figure 4 shows the denial-of-service attack.

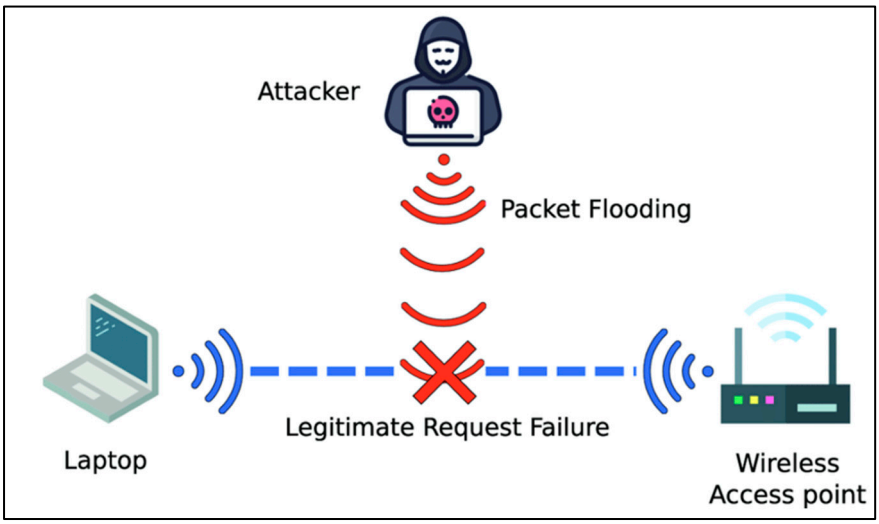

Figure 4. Example of a Denial-of-Service attack (Staddon, Loscri and Mitton, 2021).

3. Example Security-Related Technology

Security indeed is topical and central to any discussion of cloud computing, an environment that is already dynamic. In the attempt to safeguard the data from unauthorized access and to preserve Cloud security, confidentiality, integrity and availability, service providers employ numerous

 doi:10.20944/preprints202501.0494.v1

advanced security measures. These technologies have been designed to prevent potential threats such as unauthorized access, data breaches, service disruptions, and other malicious activities. This part of this discussion will focus mainly on Identity and Access Management (IAM), encryption, firewalls, Intrusion Detection Systems (IDS), and Service Level Agreements (SLAs) as the key areas embraced by today's cloud stakeholders and their customers, examining how exactly these technologies enhance cloud security and protect clients' interests.

Identity and Access Management (IAM)

Identity and Access Management (IAM) frameworks are the basis of cloud security because they control who gains access to cloud resources and what they are allowed to do with them (Singh et al., 2023; Sindiramutty, Tan, Shah, et al., 2024). IAM enables organizations to set up tight measures that limit the accessibility of some data or applications to only identified users and services. This eliminates the possibility of outsiders accessing the information, which is very important in safeguarding information.

For instance, Amazon Web Service's Identity and Access Management (IAM) allows the configuration of the roles and permissions to which a user has access for a principle of least privilege (Singh et al., 2023; Sindiramutty, Tan, & Wei, 2024). This implies that users only get an opportunity to use resources that are essential in performing their tasks, thus reducing the probability of exposing other information. Further, IAM facilitates the implementation of Multi-Factor Authentication (MFA) where a user needs to prove his identity in multiple ways before gaining access to the cloud resources (Suleski et al., 2023). This improves security and also minimizes the chances of a breach occurring.

Identity and Access Management (IAM) can help organizations make better access control and guarantee that only the permitted individuals will be able to get some data, which will help to meet such regulations as the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA). These regulations require that information and data related to the user be well protected to enhance the privacy of the users besides being able to meet the legal requirements (CE; 2023; *Legal text* 2024). By enforcing these security protocols, cloud providers ensure that organizations can securely store and handle data while maintaining privacy standards. These regulations not only prevent unauthorized access but also mitigate the risk of heavy fines and reputational damage due to non-compliance, making them a key component of cloud security strategies.

3.1. Encryption

Encryption is an important technology that makes data secure both when they are stored (Data at rest) and when they are in motion (Data in transit; Badawi et al., 2022). If an attacker has unauthorized access to the cloud resources, data stored in the cloud are encrypted and cannot be understood without the decryption key, which adds a layer of security against data loss.

For instance, Amazon Web Service uses AES-256 encryption for data stored in the Amazon S3 and for data that is transmitted through the network (Yumang et al., 2023; Waheed et al., 2024). In the same manner, Google Cloud also includes default encryption for all information, in transit and rest, thus no need for manual activation. This integrated encryption feature also contributes to the company's adherence to data protection laws across the world (Ryngaert & Taylor, 2020), thus minimizing the need to add extra layers of protection and time-consuming processes for businesses to protect users' data. Cloud providers effectively minimize the chance of data leakage and guarantee the confidentiality and integrity of data, avoiding situations when a breach results in financial or reputational losses (Li et al., 2023; Wen et al., 2023).

3.2. Firewalls and Intrusion Detection Systems (IDS)

Firewalls and Intrusion Detection Systems (IDS) are some of the critical tools that should be implemented when designing a cloud network to prevent attacks from within or outside a cloud environment. Firewalls are the security boundaries between secure internal networks and less secure external networks or between two secured networks with different levels of security (Zhou et al., 2021; Alex et al., 2022). They exclude any unauthorized traffic by only permitting the right traffic to

 doi:10.20944/preprints202501.0494.v1

pass through. On the other hand, IDS is always scanning the network traffic in the background looking for any malicious activity and threats and will raise an alarm for any unusual network traffic, which may be a sign of a breach of security (Shujat et al., 2022; Alferidah & Jhanjhi, 2020).

For instance, the Web Application Firewall (WAF) of Microsoft Azure helps protect web applications from typical attacks such as SQL injection and cross-site scripting (XSS) based on pattern matching of incoming traffic (Sumaryana, 2021; Alkinani et al., 2021). Moreover, Azure Firewall is capable of incorporating advanced threat intelligence, which means that threats are detected in real-time, and actions are taken against them without delay, which makes it a more proactive platform in terms of security.

Thus, Intrusion Detection Systems work in parallel with firewalls to identify such threats that have perhaps slipped through the firewall net or are originating from inside the cloud. For example, Google Cloud's Security Command Center serves as an IDS by constantly analyzing the flow of traffic and the structure of the network (Babbar et al., 2021). It enables it to identify activity anomalies like anomalous access and requests that can be reported to the system administrators who can then take necessary action against any prospective threats (Putra & Mutijarsa, 2021).

Another important security technology is Google Cloud's Cloud Armor, which protects against Distributed Denial of Service (DDoS) and filters out the bad traffic to the cloud infrastructure. Integrating firewalls for access control and Intrusion Detection Systems for active monitoring will enable cloud providers to achieve a strong defence system that will prevent any unauthorized attempts at accessing the data, detect any unusual behaviour, and act on such threats in the shortest time possible.

With firewalls and IDS, cloud providers can easily detect and prevent intrusions, detect anomalies and respond to threats immediately, thus enhancing the security of cloud environments and preserving the confidentiality of customer information.

3.3. Service Level Agreements (SLAs)

Service Level Agreements (SLAs) are an important factor for cloud service providers and can act as a guide of what is expected of the service providers in terms of service uptime as well as security features (Ganapathy & Joshi, 2022; Brohi et al., 2020). SLAs describe what service is to be delivered along with the availability assurances and response times for incidents, as well as the specific security commitments expected of a provider that customers will receive.

For example, Amazon Web Services SLA provides 99.99% availability of the service for crucial services like Amazon EC2 and Amazon S3 that can help customers avoid service interruption and be always available for their clients that use cloud applications (Amrullah et al., 2023; Chesti et al., 2020). This high availability is particularly useful for organizations that require consistent and reliable access to their data and applications to function and the Service Level Agreements (SLAs) ensure that AWS is held to its uptime promises. If the service level has not been achieved, AWS offers credit or service refunds to the customers as a sign of responsibility.

Like the Service Level Agreements (SLAs) provided by Google Cloud, the guarantee is that services such as Google Compute Engine and Google Cloud Storage must be up and running 99.9% of the time (Gustian et al., 2023; Dogra et al., 2021). This guarantees that the cloud resources are always available, and this is a fundamental aspect in business. Furthermore, Google Cloud's SLA defines its obligations for the protection of cloud infrastructure and points out such tasks as the physical security of the data centres and the data encryption (Mughal et al. 2024) for the data stored in the cloud and transmitted through the network, which emphasizes the provider's commitment to the security of the customer's data.

Service Level Agreements (SLAs) also have a responsibility for handling issues to do with data security and compliance. For instance, virtually all of the SLAs are likely to state that the provider will follow standard security protocols such as encryption and firewall and that data will be protected according to the current laws including the GDPR or HIPAA (Fatima-Tuz-Zahra et al., 2020). This is especially relevant for the industries regulated by laws and regulations because SLAs guarantee compliance with the law on data protection by cloud providers.

 doi:10.20944/preprints202501.0494.v1

In the same respect, Service Level Agreements make the cloud services reliable and secure because the cloud service providers guarantee their customers that required protection measures against risks for example, data leakage, unauthorized access and service disruptions are in place. A cloud provider can reassure its customers that their data is secure and that if there is a breach the cloud provider shall act by the contractual terms.

Through incorporating Identity and Access Management, Encryption, Firewalls, Intrusion Detection Systems, and Service Level Agreements these cloud providers can ensure organizations meet these compliance standards so that they are not charged steep penalties while at the same time building the much-needed customer trust. This also relieves customers' concerns that their data is being processed securely and in compliance with the law.

4. Discussion on the Impact

4.1. Benefits

Moving its operations to a cloud setup came with several key benefits for the company. The most noticeable one, however, was the fact that it is cost-efficient because it reduces maintenance costs by not having to depend on server hosting, while the company was then at its disposal to embrace a pay-as-used pricing model that only charges for how much resources they consume (Gopi et al., 2021). Financial independence was thus improved besides the reduction in operational costs. In addition to scalability, the flexibility that was enabled by the cloud architecture has thereby made it rather easy for a business to change its resources to comply with changing needs, particularly during peak hours. Because of its responsiveness, the business could adapt to the changes within its immediate business surroundings and retain peak levels of performance. Moreover, migration to the cloud increased collaboration among staff and its accessibility (Gouda et al., 2022). Team members could work better as a team regardless of their physical location, as there was greater access to data and applications, hence increasing output altogether. Another key benefit was that the strong disaster recovery solutions from the cloud provider could be implemented, thereby securing business continuity through the realization of fast data backup and restoration that are of paramount importance in mitigating risks of loss of data. Table 1 shows the benefits of cloud computing.

Table 1. Benefits of cloud computing.

Cost-Effectiveness:	• Pay-as-you-go pricing model • Reduced operational costs • Higher financial control
Improved Collaboration and Access	• Ease of access by members to data and applications • In general, increased productivity irrespective of geographical location
Scalability and Flexibility	• Resources can be scaled up/down according to demand requirements. • Any organization with a seasonal or generally fluctuating workload will find this useful.
Sustainable Environmentally Friendly	• Energy use is optimized to mean a lower carbon footprint • Centralized resources are in leaner operation processes.

4.2. Limitations

On the other hand, this transition towards cloud computing also meant several restrictions that needed consideration with due diligence. There was the issue of security where, being one among many firms in those transition periods, the company was exposed to data breaches and security gaps (Humayun et al., 2022). This therefore called for precautionary measures aside from being on the lookout for risks. Besides that, accessing applications on the cloud called for corporate operations to depend more and more on an internet connection, thereby increasing the risks of possible losses of

 doi:10.20944/preprints202501.0494.v1

connectivity. Such losses would compromise access to critical services and reduce efficiency in operational works by a great measure. This included the threat of vendor lock-in: a move to switch to a particular cloud provider raises fears about the challenges and costs involved in switching to other providers in future instances (Jhanjhi et al., 2021). In this case, as the cloud environments evolved, ensuring that the relevant compliance standards were met meant continuous vigilance and frequent auditing of ongoing concerns for the organization. Lastly, the industry regulations needed to be adhered to (Khan et al. 2022). In total, although cloud computing came with numerous advantages, it became critical for the business to manage these constraints amicably if the full benefits of its new infrastructure were to be reaped. Table 2 shows the limitations of cloud computing.

Table 2. Limitation of cloud computing.

Security and Privacy Concerns	• A breach in cybersecurity and data accompanying unauthorized access. • Compromise on sensitive data in case hosted elsewhere
Dependency on Internet Connectivity	• Increased dependence on internet connectivity in terms of leveraging cloud-based applications. • This could be said to mean potential vulnerability of operational effectiveness in the case of loss of connectivity.
Vendor Lock-In	• The cost factors and intricacies of the process of switching between different cloud providers make the process difficult.
Loss of Control Over the Infrastructure	• The infrastructure behind the cloud is controlled by the vendors. • Less customizability to meet specific organizational needs.

4.3. Future Potentials

Cloud computing is going to undergo many evolutions, whereby new technologies such as edge computing will be integrated to reduce latency by processing data closer to where it is generated and creating hybrid solutions efficiently for real-world applications. Advanced AI and machine learning in the cloud will let the business go through complex data analysis, predictive analytics, and automation with ease (Kumar et al., 2021). Another interesting promise might be quantum computing; given as a cloud service soon, that enables industries like finance or pharmaceuticals to solve very complex problems in a fraction of time. While organizations increasingly adopt multi-cloud and hybrid cloud strategies, they are combining public, private, and on-premises infrastructure for improved cost, security (Zaheer et al., 2022), and compliance needs. Automation and advanced cloud orchestration will further lessen the human element in managing cloud resources, allowing seamless scaling and monitoring (Lim et al., 2019). Further, the integration of 5G and IoT with cloud computing allows for unprecedented device connectivity, driving quicker and more reliable applications for smart cities, autonomous vehicles, and industrial automation. These movements together will widen the reach of cloud computing and further concretize its place within the digital landscape. Table 3 show future potential of cloud computing

Table 3. Future potential of cloud computing.

Integration of Edge Computing	• Data processing closer to the source reduces latency. • Hybrid solutions-a combination of cloud and edge networks for real-time needs.
Enhanced AI and ML Capabilities	• Much easier access to higher-order AI and ML tools. • Allows complex data analysis, predictive analytics, and automation.
Quantum Computing in the Cloud	• Possibilities of quantum services in the cloud. • Benefits accruable to industries requiring high-speed problem-solving-for example, finance.
Full Development of Multi-Cloud and	• Combinations of public, private, on-premises infrastructure.

 doi:10.20944/preprints202501.0494.v1

Hybrid Cloud Strategies	• Optimizes the cost with Security and Compliance, depending on specific cloud choices.

5. Discussion on Security Countermeasures

5.1. Security Countermeasures

Cloud computing has revolutionized the way organizations manage their IT infrastructure, offering flexibility, scalability, and cost savings. However, it also introduces significant security risks that must be addressed to protect sensitive data and maintain trust. Here, we will focus our discussion on existing security countermeasures while evaluating their effectiveness and exploring innovative solutions to enhance cloud security.

The Cloud Security Alliance (CSA) has identified a wide variety of threats in cloud computing environments including insecure APIs, data breaches, account hijacking, cloud setup misconfiguration, and insider threats (Cloudsecurityalliance.org, 2024; Nayyar et al., 2021). This highlights the necessity of robust countermeasures (Shah et al., 2024) to mitigate effectively the risks related to these critical areas of concern.

These vulnerabilities have been addressed by organizations through various security measures. Examples of the current countermeasures are Multi-Factor Authentication (MFA), Data encryption, regular security audits, Intrusion Detection Systems (IDS), and secure API. Starting off, Multi-Factor Authentication (MFA) offers additional security and asks users to provide two or more verification factors to access. It can be any kind of physical token or an authentication app, a notification, or an SMS. This greatly minimizes the risk of a stolen set of credentials being used against you.

On top of that, data encryption is one additional strong countermeasure that helps to upkeep the security of the cloud. This encrypts data for both rest and in transit, so if data was intercepted or accessed without authorization, you are unable to read the data until proper decryption keys are authorized (Shah et al., 2022). It is very important to protect sensitive data from breaches and information compromise. Regular security audits also help organizations discover vulnerabilities and ensure compliance with industry standards and legislation. This practice can help you discover the setup misconfiguration and the security gaps before they can get exploited.

Intrusion Detection Systems (IDS) will target suspicious or unusual activities by monitoring network traffic for patterns and behaviours indicative of potential threats. An IDS works by analyzing patterns and behaviors, allows administrators to know when there is a possibility of intrusion and take timely measures in place. Lastly. Strong authentication and access controls on an API help prevent and reduce the impact of unauthorized access. This means that regular testing of API interfaces for their vulnerability is also an important thing and should be performed (at least) alongside internal security audits.

6. Proposed Countermeasures (Defense Solution)

These countermeasures that are considered effective are not entirely perfect and foolproof. For example, social engineering attacks can bypass MFAs and data encryption heavily depends on the correct key management. Furthermore, misconfigurations tend to continue to be a problem, especially because people will make mistakes, and many organizations simply do not have the expertise necessary to configure cloud environments securely. The rapid evolution of cloud services creates a challenge that makes it difficult to keep up with the latest vulnerabilities and threats for an IT team (Singh and Saroha, 2018; Sharma et al., 2021). A lack of visibility and control, which is often common in the dynamic nature of cloud environments, makes it difficult to maintain a uniform level of security (Behera et al., 2023).

To enhance the security of the cloud further, organizations should consider the following innovative countermeasures:

AI-Powered Threat Detection: By applying artificial intelligence (AI) to the analysis of vast amounts of real-time data, threat detection capabilities can be significantly improved in identifying anomalies characteristic of potential attacks. As machine learning algorithms gain popularity, and

 doi:10.20944/preprints202501.0494.v1

organizations become more reliant on them, there is a greater reliance on the companies that provide those services to keep up with new cyber threats as they emerge, and organizations want to stay on top (Singhal et al., 2020). Enhanced User Education and Training Programs: Training employees on security best practices in regular training sessions can cut the odds of phishing attacks and insider threats by quite a lot. Ongoing education programs need to occur in organizations to train staff to fight against new threats and to know what to do when a security risk occurs.

Zero-Trust Architecture: In adopting a Zero Trust model, no user or device is trusted by default regardless of whether they are on or off the network perimeter. This approach necessitates real-time verification of users' identities, and a finely tuned access control model based on users' roles and activities. One way to mitigate the impact of a potential breach, and to reduce the attack surface, is via Zero Trust.

Automated Configuration Management: When you're building and managing your cloud resources and automating config management, you can use automated tools to make sure you're setting things up the way you should. With these tools, they can alert you to any deviations from the configured status, so you can take immediate corrective action. Detailed Incident Response Plans: The best practice is to develop detailed incident response plans along with predefined roles and responsibilities so that organisations can respond swiftly and efficiently to security incidents. These plans should be regularly drilled under different scenarios to test them.

Sustainability in Cloud Security: As organizations focus on security, they should also consider the environmental impact of their operations. Storage optimization and adoption of energy-saving algorithms as well as green cloud solutions can help marry security with sustainability goals.

Organizations that deploy these advanced countermeasures alongside constant awareness of security trends, can greatly improve the security of their cloud-used environments (ISACA, 2019). Security policies and procedures must always be reviewed, updated and modified to reflect changing threats and evolving technology. Also, organisations should consider collaborating with security professionals with experience of working with providers able to provide cloud security services to get through the labyrinth of cloud security as well as protect what are purely valuable assets.

7. Conclusions

The report highlights the growing importance of implementing robust cybersecurity measures for cloud services to address the numerous security issues and challenges as they are vital in our everyday lives. To provide insight into the issue of addressing security challenges, the report delves into security-related technologies such as IAM, Firewalls, IDS, etc, going into detail on the components, the processes and how security-related technologies will be able to neutralize the threats to give a comprehensive understanding on security-related technologies. The following section has allowed us to understand the impact of utilizing cloud services, specifically the benefits such as cost-effectiveness, the scalability and limitations of the cloud services such as the dependence on network connectivity, and data privacy concerns. A proposed framework of security countermeasures was developed on the foundational knowledge of security-related technologies provided earlier in the report. Key technologies such as IAM, firewalls, encryption, and IDS are known to be highly effective in guaranteeing a safe and secure cloud environment. To prepare for future emerging threats, innovative technologies such as AI-powered threat detection, zero-trust architecture, and automated configuration management should be focused on and integrated to further improve the current security-related technologies thus further reducing vulnerabilities in the cloud infrastructure. By leveraging these security-related technologies and adopting the multi-layer authentication approach, organizations can improve the resilience of the cloud infrastructure significantly, paving the way for a secure digital future.

 doi:10.20944/preprints202501.0494.v1

References

1. Achar, S. (2022). CLOUD COMPUTING FORENSICS CLOUD COMPUTING FORENSICS. *International Journal of Computer Engineering and Technology (IJCET)*, [online] 13(3), pp.1–10. doi:https://doi.org/10.17605/OSF.IO/9N64K.
2. Achar, S. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. *Zenodo (CERN European Organization for Nuclear Research)*. [online] doi:https://doi.org/10.5281/zenodo.7084251.
3. Acta Informatica Pragensia (no date) *Improving privacy-preserving healthcare data sharing in a cloud environment using hybrid encryption, Acta Informatica Pragensia*. Available at: https://aip.vse.cz/artkey/aip-202203-0006_improving-privacy-preserving-healthcare-data-sharing-in-a-cloud-environment-using-hybrid-encryption.php
4. Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, [online] 15(02), pp.148–167. doi:https://doi.org/10.4236/jis.2024.152010.
5. 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
6. 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
7. Al-Ghuwairi, A.-R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A. and Algarni, A. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. *Journal of Cloud Computing*, [online] 12(1). doi:https://doi.org/10.1186/s13677-023-00491-x.
8. 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
9. Alsirhani, A., Ezz, M. and Mostafa, A. (2022) *Advanced authentication mechanisms for identity and Access Management in cloud computing*, *Tech Science Press*. Available at: https://www.techscience.com/csse/v43n3/47698
10. Amrullah, A., Nugroho, A. and Ramadhan, Z. (2023) Perbandingan Kinerja web server Pada PENYEDIA layanan cloud microsoft azure dan amazon web services, Jurnal Informatika Teknologi dan Sains (Jinteks). Available at: https://jurnal.uts.ac.id/index.php/JINTEKS/article/view/2487.
11. 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
12. Ariyanto, Y., Harijanto, B., Firdaus, V.A.H. and Arief, S.N. (2020). Performance analysis of Proxmox VE firewall for network security in cloud computing server implementation. *IOP Conference Series: Materials Science and Engineering*, 732(1), p.012081. doi:https://doi.org/10.1088/1757-899x/732/1/012081.
13. 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
14. 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
15. 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

16. 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
17. 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
18. Badawi, A.A. et al. (2022) OpenFHE: Open-source fully homomorphic encryption library, New Jersey Institute of Technology. Available at: https://researchwith.njit.edu/en/publications/openfhe-open-source-fully-homomorphic-encryption-library (Accessed: 29 November 2024).
19. Behera, S. R., Panigrahi, N., Bhoi, S. K., Sahoo, K. S., Jhanjhi, N. Z., & Ghoniem, R. M. (2023). Time series-based edge resource prediction and parallel optimal task allocation in mobile edge computing environment. *Processes*, *11*(4), 1017.
20. 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
21. Brown, S. (2024). *Top Cloud Security Issues and Risks to Be Aware of in 2023 | StrongDM*. discover.strongdm.com. Available at: https://www.strongdm.com/blog/cloud-security-issues-risks
22. CE;, M.M. (2023) Ai Chatbots, Health Privacy, and challenges to HIPAA compliance, JAMA. Available at: https://pubmed.ncbi.nlm.nih.gov/37410450/ (Accessed: 29 November 2024).
23. 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
24. Cloud Native Wiki by aqua (2024) 'Cloud Security Tools', Cloud Native Wiki by aqua. Available at: https://www.aquasec.com/cloud-native-academy/cspm/cloud-security-tools/
25. Cloudsecurityalliance.org. (2024). *Top Threats to Cloud Computing 2024 | CSA*. [online] Available at: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024 [Accessed 29 Nov. 2024].
26. CloudZero (2024) 'Cloud computing statistics', CloudZero. Available at: https://www.cloudzero.com/blog/cloud-computing-statistics/ (Accessed: 12 November 2024).
27. Deemer, B. (2023). *What Are the Security Risks of Cloud Computing?* www.auditboard.com. Available at: https://www.auditboard.com/blog/what-are-the-security-risks-of-cloud-computing/
28. 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
29. E Balamurugan, Abolfazl Mehbodniya, Elham Kariri, Yadav, K., Kumar, A. and Haq, M.A. (2022). Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN). *Pattern Recognition Letters*, [online] 156, pp.142–151. doi:https://doi.org/10.1016/j.patrec.2022.02.013.
30. Edwards, J. (2024). *11 top cloud security threats*. CSO Online. Available at: https://www.csoonline.com/article/555213/top-cloud-security-threats.html.
31. Ej-eng.org. (2024). *View of IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations*. [online] Available at: https://www.ej-eng.org/index.php/ejeng/article/view/3074/1425 [Accessed 13 Nov. 2024].
32. 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
33. Ganapathy, D.N. and Joshi, K.P. (2022) Divya n Ganapathy, IEEE Transactions on Services Computing. Available at: https://ebiquity.umbc.edu/paper/html/id/1012/A-Semantically-Rich-Framework-to-Automate-Cloud-Service-Level-Agreements (Accessed: 29 November 2024).
34. Gaur, L., & Jhanjhi, N. Z. (Eds.). (2023). *Metaverse applications for intelligent healthcare*. IGI Global.

35. 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
36. 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
37. Gustian, D. et al. (2023) IMPLEMENTASI automation deployment pada google cloud compute VM menggunakan terraform, INOVTEK Polbeng - Seri Informatika. Available at: https://ejournal.polbeng.ac.id/index.php/ISI/article/view/3095 (Accessed: 29 November 2024).
38. HAProxy Technologies (2024). *What is rate limiting?* HAProxy Technologies. Available at: https://www.haproxy.com/glossary/what-is-rate-limiting
39. Hossein Abroshan (2021). A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Computer Science and Applications*, [online] 12(6). doi:https://doi.org/10.14569/ijacsa.2021.0120604.
40. 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
41. 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
42. Putra and K. Mutijarsa (2021) Designing information security risk management on Bali ... Available at:https://www.researchgate.net/publication/351646740_Designing_Information_Security_Risk_Management_on_Bali_Regional_Police_Command_Center_Based_on_ISO_27005 (Accessed: 29 November 2024).
43. Ieee.org. (2024). *IEEE Xplore Full-Text PDF:* [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8863330 [Accessed 13 Nov. 2024].
44. ISACA. (2019). *Evolving Threats to Cloud Computing Infrastructure and Suggested Countermeasures*. [online] Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/evolving-threats-to-cloud-computing-infrastructure-and-suggested-countermeasures [Accessed 29 Nov. 2024].
45. Ismail, U.M. and Islam, S. (2020). A unified framework for cloud security transparency and audit. *Journal of Information Security and Applications*, [online] 54, pp.102594–102594. doi:https://doi.org/10.1016/j.jisa.2020.102594.
46. Jadama, A.F., Islam, M., Touray, M.K., Sharma Durba and Springer, A. (2024). Enhancing IoT Security and Privacy in the Cloud: A Framework for Secure Data Transmission and Storage. [online] doi:https://doi.org/10.13140/RG.2.2.15055.09128.
47. 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
48. 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
49. K. Samunnisa, Kumar, V. and K. Madhavi (2022). Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods. *Measurement Sensors*, [online] 25, pp.100612–100612. doi:https://doi.org/10.1016/j.measen.2022.100612.
50. Khan, A., Jhanjhi, N. Z., & Sujatha, R. (2022). Emerging Industry Revolution IR 4.0 Issues and Challenges. In *Cyber Security Applications for Industry 4.0* (pp. 151-169). Chapman and Hall/CRC.
51. 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
52. Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 29 November 2024).
53. Li, W.W., Leung, A.C.M. and Yue, W.T. (2023) Where is it in information security? the Interrelationship among IT investment, security awareness, and data breaches, MIS Quarterly. Available at:

https://misq.umn.edu/where-is-it-in-information-security-the-interrelationship-among-it-investment-security-awareness-and-data-breaches.html (Accessed: 29 November 2024).

54. 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
55. MacLean, K. (2024). Understanding SLAs For Cloud And Bare Metal Services. [online] DataBank | Data Center Evolved. Available at: https://www.databank.com/resources/blogs/understanding-slas-for-cloud-and-bare-metal-services/
56. 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
57. Microsoft.com. (2024). *What is CSPM? | Microsoft Security*. Available at: https://www.microsoft.com/en-my/security/business/security-101/what-is-cspm
58. Mission Cloud (2024) 'Top 5 Cloud Security Challenges of 2024 and How to Mitigate Them', Mission Cloud. Available at: https://www.missioncloud.com/blog/top-5-cloud-security-challenges-of-2024-and-how-to-mitigate-them (Accessed, 12 November 2024).
59. Mughal, M. A., Ullah, A., Cheema, M. A. Z., Yu, X., & Jhanjhi, N. Z. (2024). An intelligent channel assignment algorithm for cognitive radio networks using a tree-centric approach in IoT. *Alexandria Engineering Journal*, *91*, 152-160.
60. 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
61. None Zein Samira, None Yodit Wondaferew Weldegeorgise, None Olajide Soji Osundare, Oke, H. and Coelis, R. (2024). Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*, 12(1), pp.043–055. doi:https://doi.org/10.30574/msarr.2024.12.1.0146.
62. Proofpoint (2021). *What Is Cloud Security?* Available at: https://www.proofpoint.com/us/threat-reference/cloud-security.
63. Rajeswari Baby Natchiar M (2023). *What Is A Security Misconfiguration? - Prophaze Web Application Security*. Prophaze Web Application Security. Available at: https://prophaze.com/2023/04/25/security-misconfiguration/
64. Rana, P., Batra, I., Malik, A., Agbotiname Lucky Imoize, Kim, Y., Pani, S.K., Goyal, N., Kumar, A. and Rho, S. (2022). Intrusion Detection Systems in Cloud Computing Paradigm: Analysis and Overview. *Complexity*, [online] 2022(1). doi:https://doi.org/10.1155/2022/3999039.
65. 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
66. Ryngaert, C. and Taylor, M. (2020) The GDPR as Global Data Protection Regulation?: American Journal of International law, Cambridge Core. Available at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688 .
67. Sajid, H. (2023). *How to Prevent Data Loss in Cloud Computing?* V2 Cloud. Available at: https://v2cloud.com/blog/how-to-prevent-data-loss-in-cloud-computing
68. Sana, M.U., Li, Z., Javaid, F., Hannan Bin Liaqat and Ali, M.U. (2021). Enhanced Security in Cloud Computing Using Neural Networks and Encryption. *IEEE Access*, [online] 9, pp.145785–145799. doi:https://doi.org/10.1109/access.2021.3122938.
69. Seid, E., Nazifa, M., Gupta, S., Popov, O. and Blix, F. (2024). Security and SLA Monitoring for Cloud Services. *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering*, [online] pp.537–546. doi:https://doi.org/10.5220/0012690800003687.
70. 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

71. 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
72. Shah, I. A., Jhanjhi, N. Z., & Rajper, S. (2024). Use of Deep Learning Applications for Drone Technology. In *Cybersecurity Issues and Challenges in the Drone Industry* (pp. 128-147). IGI Global.
73. Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). IoT Devices in Drones: Security Issues and Future Challenges. In *Cybersecurity Issues and Challenges in the Drone Industry* (pp. 217-235). IGI Global.
74. 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
75. Shujat, M. et al. (2022) (PDF) Enterprise Network Infrastructure Malicious Activity Analysis. Available at: https://www.researchgate.net/publication/364760019_Enterprise_Network_Infrastructure_Malicious_Activity_Analysis (Accessed: 29 November 2024).
76. Shukla, D.K., Dwivedi, V.K.R. and Trivedi, M.C. (2020). Encryption algorithm in cloud computing. *Materials Today Proceedings*, [online] 37, pp.1869–1875. doi:https://doi.org/10.1016/j.matpr.2020.07.452.
77. 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
78. 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
79. 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
80. 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
81. 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
82. 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
83. Singh, C., Thakkar, R. and Warraich, J. (2023) IAM identity access management-importance in maintaining security systems within organizations, European Journal of Engineering and Technology Research. Available at: https://www.ej-eng.org/index.php/ejeng/article/view/3074 (Accessed: 29 November 2024).
84. 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
85. Staddon, E., Loscri, V. and Mitton, N. (2021). *Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey*. Available at: https://www.researchgate.net/figure/llustration-of-a-Denial-of-Service-attack_fig3_353723022
86. Suleski, T. et al. (2023) A review of multi-factor authentication in the internet of healthcare things, Digital health. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC10214092/ (Accessed: 29 November 2024).
87. Sumaryana, Y. (2021) Peningkatan Keamanan Aplikasi web menggunakan web application firewall (WAF) Pada Sistem Informasi manajemen kampus terintegrasi, Jurnal ICT : Information Communication & Technology. Available at: https://www.academia.edu/100293206/Peningkatan_Keamanan_Aplikasi_Web_Menggunakan_Web_Application_Firewall_WAF_Pada_Sistem_Informasi_Manajemen_Kampus_Terintegrasi

88. Usman Inayat, Farzan, M., Mahmood, S., Muhammad Fahad Zia, Hussain, S. and Fabiano Pallonetto (2024). *Insider threat mitigation: Systematic literature review*. *Ain Shams Engineering Journal*. Available at: https://www.sciencedirect.com/science/article/pii/S209044792400443X
89. 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
90. 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
91. Wiz (2024) 'The Shared Responsibility Model Explained', Wiz Academy. Available at: https://www.wiz.io/academy/shared-responsibility-model (Accessed: 12 November 2024).
92. Yadav, S.S., Kalaskar, K. and Dhumane, P. (2023). *A Comprehensive Survey of IoT- Based Cloud Computing Cyber Security*. Available at: https://www.researchgate.net/figure/Graphical-Representation-of-an-account-hijacking-attack-15_fig2_367237358
93. Yumang, A.N. et al. (2023) IOT-based fire mitigation and detection system with AES-256 encryption and Android application, CoLab. Available at: https://colab.ws/articles/10.1109%2Fisstc59603.2023.10281116 (Accessed: 29 November 2024).
94. Zaheer, A., Tahir, S., Humayun, M., Almufareh, M. F., & Jhanjhi, N. Z. (2022, November). A novel Machine learning technique for fake smart watches advertisement detection. In *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)* (pp. 1-5). IEEE.
95. Zhou, Y., Hu, Z. and Li, F. (2021) Searchable public-key encryption with cryptographic ... Available at: https://www.researchgate.net/publication/353110449_Searchable_Public-Key_Encryption_with_Cryptographic_Reverse_Firewalls_for_Cloud_Storage