Article

Not peer-reviewed version

Advanced Cloud Security Frameworks: Tackling Evolving Threats and Ensuring Data Integrity

Chin Jun Kiat , Wong Ping Chen , Tan Zhaw Yaen , Jay Lieow Yu Jye , Ooi Yan Min , Rakibul Hasan , Pan Yi Bing , Ng Zhao Hern , Muhammad Mahin Ali , Tan Jun Rou , Alaaeldeen Adil Eltayeb Abdelnour , Siva Raja Sindiramutty *

Posted Date: 9 January 2025

doi: 10.20944/preprints202501.0745.v1

Keywords: Cloud Computing Security; Data Breach Prevention; Advanced Threat Detection; Zero-Trust Architecture; Quantum-Resistant Encryption

Article

Advanced Cloud Security Frameworks: Tackling Evolving Threats and Ensuring Data Integrity

Chin Jun Kiat, Wong Ping Chen, Tan Zhaw Yaen, Jay Lieow Yu Jye, Ooi Yan Min, Rakibul Hasan, Pan Yi Bing, Ng Zhao Hern, Muhammad Mahin Ali, Tan Jun Rou, Alaaeldeen Adil Eltayeb Abdelnour and Siva Raja Sindiramutty

0369163@sd.taylors.edu.my, 0365039@sd.taylors.edu.my, zhawyaen.tan@sd.taylors.edu.my, jayyujye.lieow@sd.taylors.edu.my, 0376107@sd.taylors.edu.my, rakibulhasan@sd.taylors.edu.my, 0365361@sd.taylors.edu.my, zhaohern.ng@sd.taylors.edu.my, muhammadmahinali@sd.taylors.edu.my, junrou.tan@sd.taylors.edu.my, 0368738@sd.taylors.edu.my, magan.shiva91@gmail.com

Abstract: Cloud computing is a public and private data center that provides customers with a single platform across the Internet. Users can upload information and data to the cloud space and query and modify it at will without occupying the memory of their own devices. It is an evolving computing paradigm that stores data and information closer to end users to improve response time and save transmission capacity. Cloud computing has received widespread attention due to its affordability and high-quality services. Despite the many benefits of cloud computing, its security issues are still considered a big challenge. In the cloud computing security landscape, a three-tier model is divided, namely, IaaS, PaaS, and SaaS. The results show that user data tampering and leakage are one of the most discussed topics in the selected literature. Other identified security risks are related to data intrusion and data storage in cloud computing environments. Our research report will discuss in detail the working principles of security-related technologies, as well as the advantages, limitations, and future potential of cloud computing. The results also reveal some recommendations that need to be implemented in future work to ensure data confidentiality, integrity, and availability.

Keywords: Cloud Computing Security; Data Breach Prevention; Advanced Threat Detection; Zero-Trust Architecture; Quantum-Resistant Encryption

1.0. BACKGROUND

Cloud security is that branch of cybersecurity that principally concentrates on protection features concerning cloud data, applications, and services. With all those organizations from different industrial streams leaning mostly towards cloud infrastructures for the storage and running of highly critical applications, the requirement for effective cloud security grows with each passing day. In contrast to traditional IT infrastructure, where data lives on-premises, controlled by an organization, through on-prem-based servers, cloud is built upon remote servers controlled by third-party providers such as Amazon Web Services (AWS), Microsoft Azure and the Google Cloud. Cloud platforms enable organizations to store tremendous amounts of data, run applications at scale, and provide global access to services (What are the benefits of Cloud Computing, 2024). Nonetheless, cloud environments come with their own set of security challenges, which has made the subject of cloud security very relevant for organizations today.

The cloud systems are more scalable, adaptive, and economical as compared to other ways of handling big data, which has led to increased popularity. Moving to cloud has liberated many businesses from the cost and the hassle of running and maintaining physical data centres - employees can focus their skills in areas that matter more to core business (Why is the cloud so cost-effective? 2023; Ananna et al., 2023). Also, cloud computing has provided organizations with rapid responses when needs change quickly with the increased demand for remote work and digital offerings.

 doi:10.20944/preprints202501.0745.v1

However, with these benefits come critical security concerns. The very nature of cloud data, accessible via the internet, makes it susceptible to more attacks than that contained in isolated, on-premises systems (Attacks from the Cloud, 2024; Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023). It also means that securing data against illegal access, hacks, and cyberattacks on the cloud needs its own security solutions and all new ways of approaching security.

Security issues relating to the cloud mainly focus on securing data. Data housed on a cloud platform can reside across numerous data centers, often strewn throughout different geographical locations and even countries. The implications of this on data sovereignty and regulatory compliance are multifold, since there is very little overlap in the data protection laws across jurisdictions. In sectors where there are multiple compliance guidelines like HIPAA and PCI DSS, just having the proper security tools mitigates the business risk caused by exposed sensitive data (Fandrick, 2024). The organizations will operate within legal and ethical bounds of these laid-down criteria, with non-compliances resulting in hefty penalties and loss of prestige. Some of the critical cloud security solutions that play an essential role in meeting regulatory standards, ensuring data confidentiality and integrity, are security solutions on the cloud with encryption, data masking, and safe ways of data storage methods (Richman, 2023; Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023).

Another key pillar of cloud security is access to cloud resources. While cloud platforms have allowed employees, partners, and other stakeholders access to corporate data and applications from almost any location with access to the internet, in return, this has created flexibility and productivity but may open new vectors to possible vulnerabilities (Media, 2023; Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023). For instance, in case an employee works from a remote location, connecting to the cloud via public Wi-Fi in an unencrypted coffee shop, sensitive information becomes open to unauthorized persons. Finally, businesses may utilize contractors and travel remote teams who access from their phones or other personal devices with possibly out of date security layers.

Apart from data protection, access control and threat mitigation, a cloud security solution can help keep your business running. Natural or man-made disasters strike suddenly, and if the organization does not have enough protection against such incidents, its entire data set might be compromised or lost. The cloud security solutions include backup technologies that establish duplicate replicas of data and systems in data centers far from each other, enabling the organizations to bring back their operations swiftly, even during a catastrophic system failure (What is Cloud Backup? How It Works, Benefits and Best Practices, 2024; Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023). Which is critical to drive customer confidence and sustain business operations in the face of a growing volatile threat landscape.

To summarize, cloud security is the bedrock of modern-day cloud computing. It provides privacy, correctness, availability of data, helps in meeting regulatory requirements, enables remote access safely and secures the entire network infrastructure against a wide variety of cyber-attacks. To organizations leveraging cloud computing as a stepping stone toward accelerated digital transformation, cloud security is both a defense mechanism and a strategic enabler; it empowers them to pursue innovation aggressively without any compromise in risk management processes. This rapid expansion in the adoption of cloud will be complemented by an increased demand for advanced security capabilities that keep pace with evolving threats and, in the end, assure a secure, resilient cloud environment-to their benefit and that of their customers.

 doi:10.20944/preprints202501.0745.v1

2.0. DETAILED DISCUSSION ON HOW SECURITY-RELATED TECHNOLOGY WORKS

2.1. Component

Introduction to the Components in Cloud Computing Security

Securement of cloud environments is necessary since, as with any other environment, the cloud has its threats as well. Cloud-based infrastructures face a variety of risks, including data leaks, unauthorised access, cyber threats, etc. Yet, with the flexible and scalable nature of cloud computing, new challenges also arose as threats evolved, such as data leaks, lateral movement attacks, insider threats, etc. This part will present the main security components designed in cloud computing technologies and provide explanations of how they might help lose cloud environments, including in detail what functions each of them may perform.

The Core Components of Cloud Security

Identity and Access Management (IAM) is one of the basic components in cloud security that manages and organises cloud resource users so there is only a valid and permitted individual who manages sensitive systems and data. Many technologies are involved in IAM, including some frameworks like Multi-Factor Authentication (MFA), Single Sign-On (SSO), or Role-Based Access Control (RBAC); such technologies integrate IAM components into an efficient secure access infrastructure in the cloud. This component maintains a balance between the accessibility of the information and the degree of limitation of access to it. However, in such circumstances, the creation and management of users and enterprises are always difficult, if not impossible, to implement, unless there are central policies, audit and monitoring schedules, and frameworks for governance of identity available within the enterprise. (Mohammed, I.A. 2019; Hussain et al., 2024).

Data encryption is one other key element in protecting data when it is not meant to be seen by unauthorised people, during its transfer, or when it is stored. Other than protecting data in the cloud, data encryption can be done through symmetric and asymmetric techniques, which in turn protects data within the cloud. Such measures are necessary to protect sensitive information from interception or access by people or systems who are not authorised to use that information, in this case protecting the privacy of data (Saleh et al,. 2020, Muzafar et al., 2021) as well as meeting the legal requirements for the data. Treating and sustaining encryption keys does come with certain limitations because the keys must be kept safe and only be accessed by authorised systems (Li et al,. 2021) and personnel, which more often than not requires high levels of key management practices to ensure data confidentiality (Hidayat, T., & Mahardiko, R. 2020; Jun et al., 2024).

Network security is the protective layer that controls data traffic in the cloud environment against unauthorised users and cyber threats. Network security is a combination of firewalls, virtual private networks (VPNs), intrusion detection systems, and intrusion prevention systems, which are important because they protect networks from dangers and manage attacks. In the context of data security, network security is also beneficial in the aspect of prevention, as it aids in, in most cases, preventing breaches from occurring in the first place by layering different defences and monitoring constantly (Fatima-Tuz-Zahra et al., 2020). Nevertheless, it is important to mention that providing comprehensive network security is not simple because of the inherent dynamics of cloud environments, which typically call for active monitoring (Gill et al., 2021) and determination of necessary responses to new network setups. (Sabyasachi Pramanik, Debabrata Samanta, M. Vinay, Abhijit Guha 2022; Manchuri et al., 2024).

Upon detection, endpoint security aims at securing devices that reach out to the cloud services. This is important, especially in organisations that have BYOD policies. This component combines Endpoint Detection and Response (EDR) technology as well as antivirus software to secure all devices that connect to the cloud. Endpoints must be secured because, if they are compromised, they are the first targets, and subsequently, the entire cloud infrastructure is at risk. The presence of multiple

 doi:10.20944/preprints202501.0745.v1

types of devices for usage increases the level of complexity involved in managing and securing devices because they require constant upgrades and vigorous vulnerability management to all the operating systems in place (Dave Gruber, 2024; Ravichandran et al., 2024).

However, access point and data transmission security are not perimeter-defined because application security also falls in the same category since it tries to eliminate possible vulnerabilities and potential exploitation of the cloud applications, hence is one of the core elements of cloud security. Organisations can secure their applications by deploying Web Application Firewalls (WAFs) alongside automated vulnerability scanning tools, or the more powerful combination of both. Application security deserves a lot of attention, as the cloud-native application can be one of the targets of cybercriminals (Gopi et al., 2021). The problem, however, is staying abreast of the newest security issues and vulnerabilities, which call for regular supervision and prompt action.

Finally, compliance and monitoring help in confirming the compliance it controls in all regulatory requirements and tracking the environment for possible security threats in an automated way. Compliance is encouraged through regulations such as the General Data Protection Regulation and ISO 27001 standard; security information and event management (SIEM) systems; and any audit log that facilitates monitoring in real-time. Compliance and monitoring are significant in ensuring that legal and regulatory requirements are not contravened and that potential threats are detected early (Gouda et al., 2022). Thus, even though continuous compliance and effective threat monitoring are possible, they are expensive, requiring a skilled workforce and sophisticated monitoring measures.

Integration Of Components for Comprehensive Cloud Security

The hardware integration of these components provides cloud security consolidation to achieve a multi-layered defence strategy for the architecture. IAM controls who can access the information; encryption ensures that the information is stored; and the real-time security of the network ensures that attacks are current. Meanwhile, endpoint and application security aim at vulnerability at the device and application level, respectively, while compliance and monitoring (Srinivasan et al,. 2021) ensure there is a standard and an anomaly can be detected whenever it occurs. All these together improve security posture; however, the integration requires a lot of coordination, regular changes, and compatibility testing to ensure that optimal defence architecture is in place.

These components are essential in enhancing the overall security of the cloud environment. Identity and Access Management grants access based on approval only, while encryption prevents unauthorised access to information. Network security monitors the traffic (Sama et al., 2022), endpoint security protects the devices, application security protects the weaknesses of the applications, and compliance and monitoring make sure the laws are followed. These components, when put together, create a strong security infrastructure that is required for the protection of the cloud environments. This segment creates an avenue for further debates on the implications and measures that are necessary for cloud security

2.2. Process

The fundamental basis of cloud computing service models can be summed up with the notion popularized in the IT industry as ‘shareable’, ‘computationally on-demand’, and ‘Internet-based’ resources. Customers purchase rights of usage of an online collection of various resources including computation, storage and network, located on servers controlled by the service providers.

Another advantage that comes with cloud computing of course is that you only pay for what you use. This helps organizations to grow faster and at a cheaper rate than they could if they had to acquire and own their own brick and mortar data centers and computers. In other words, cloud computing uses a network whether the internet to connect customers to an environment called cloud and where they can demand and use leased computing resources. All the communication processes involve a central server through which the client device or hardware communicates with the server to exchange data (Humayun et al., 2022). Security and privacy features are common elements used

 doi:10.20944/preprints202501.0745.v1

for maintaining such data personal and secure. Indeed, cloud computing design conceptually cannot be a one-to-one replication. What can be effective for another organization may not necessarily be effective when applied to another organization let alone your kind of business needs. In addition, the cloud flexibility /versatility differentiator, which enables a business to scale up or down, depending on the market or measurement (Ranger, 2022b; Seng et al., 2024). Deployment models of cloud computing can be categorized into three, namely private cloud, public cloud and the hybrid cloud.

Private Cloud

Private cloud refers to access of computer services through Own Internet Technology network for the entity's use. A private cloud is also referred as internal cloud, enterprise or corporate cloud is generally managed internally and it is closed to all other outsiders. Private cloud computing enjoys the characteristics of public cloud, self-service, scalability and elasticity and more control, security and customization. Business firewalls and internal hosting of private clouds enhance the security since the important information cannot be accessed by third party cloud providers. Another drawback that can be associated with private cloud implementation is that all data center management is on the organization's side, so all necessary work can be rather resource-demanding (Ot, 2023; Jhanjhi et al., 2021).

Public Cloud

Public cloud can be defined as the computer services that are available on the internet by a third-party supplier. Public clouds on the other hand can be used by anyone or even be purchased by anyone unlike the private clouds. These services may be offered gratis or whenever the customer wishes so; generally, customers pay only what they used, be it CPU cycles, storage or bandwidth. This is mainly because the cloud service provider offers to host and manage the system, so organizations do not incur costs in the procurement, installation and maintenance of on-premise facilities. They also offer the feature and RAM and variable bandwidth, thus helping enterprises to flexibly increase their storage needs (Ot, 2023; Sindiramutty et al., 2024).

Hybrid Cloud

Public and private clouds blend to form other clouds known as hybrid clouds. The hybrid cloud strategy model offers an opportunity to transfer workloads between private and public clouds according to computation and pricing requirements. During the variations in demand for computing and processing, hybrid cloudOpens a new window that must allow organizations to connect their on-premises infrastructure to public cloud but ensures that data does not go through third-party data centers (Kumar et al., 2021). It further means that in a hybrid cloud the businesses pay for the resources that are momentarily in use and not the ones that are used rarely and which when used one has to wait for a long time to be served. In summary, a hybrid cloud comes with the opportunities of a public cloud but with no risk (Ot, 2023; Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024).

Cloud computing may be classified into three delivery models which are IAAS, PAAS and SAAS.a) IaaS (Infrastructure as a Service) ublic cloud and private cloud characteristics. The "best of both worlds" cloud concept enables the migration of workloads between private and public clouds as computation and pricing needs change. When the demand for computing and processing varies, hybrid cloudOpens a new window that enables organizations to extend their on-premises infrastructure to the public cloud to manage the overflow while guaranteeing that no third-party data centers have access to their data.In a hybrid cloud approach, businesses only pay for the resources they use momentarily, rather than purchasing and maintaining resources that may not be used for a long time. In summary, a hybrid cloud provides the benefits of a public cloud but without the security dangers (Ot, 2023; Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024).

Cloud computing may be divided into three service models which are IaaS, PaaS, and SaaS.

 doi:10.20944/preprints202501.0745.v1

a) Iaas (Infrastructure-as-a-Service)

In this model, a business hires the space on the servers and the storage it needs from a cloud provider. They then use the cloud infrastructure to build their applications into what they are today. IaaS is like renting a piece of land with blank space to construct anything one would wish to construct provided they must supply their own mechanical tools set. Some of the IaaS providers are; DigitalOcean, Google Compute Engine, and OpenStack.b) PaaS (Platform as a Service) bine public cloud and private cloud characteristics. The "best of both worlds" cloud concept enables the migration of workloads between private and public clouds as computation and pricing needs change. When the demand for computing and processing varies, hybrid cloudOpens a new window that enables organizations to extend their on-premises infrastructure to the public cloud to manage the overflow while guaranteeing that no third-party data centers have access to their data.

In a hybrid cloud approach, businesses only pay for the resources they use momentarily, rather than purchasing and maintaining resources that may not be used for a long time. In summary, a hybrid cloud provides the benefits of a public cloud but without the security dangers (Ot, 2023; Lim et al., 2019).

b) PaaS (Platform-as-a-Service)

In this model companies or people in this paradigm do not purchase hosted applications; they purchase what is needed to build their own application. PaaS suppliers offer all facilities necessary for creating an application with tools, infrastructure, and operating systems available through the Internet. PaaS might be described as analogues to leasing all the tools and equipment needed to construct a house but not the house itself. Some of the PaaS are heroku and microsoft Azure according to Aweda (2024).

c) SaaS (Software-as-a-Service)

SaaS apps are hosted on cloud servers and accessed via the Internet, rather than being installed on the user's device. SaaS is similar to renting a house, the landlord maintains the property, while the renter mostly uses it as if they were the owner. SaaS apps include Salesforce, MailChimp, and Slack (Davis, 2022; Sindiramutty et al., 2024).

2.3. Threat

A cloud system can face many threats as it is hosted and used over the internet. Below is a list of potential threats to the security of cloud computing systems that can cause breaches as well as damages to a cloud.

1. **Data Breaches**: Unauthorised access to sensitive data or theft of data stored in the cloud can lead to information theft or misuse. (SentinelOne, 2024)
2. **Insider Threats**: Malicious actions and use of resources by individuals within the organisation with access to critical systems and data. (SentinelOne, 2024)
3. **Account Hijacking**: Unauthorised access to accounts through identity theft, phishing, or social engineering or other ways and use of such accounts. (SentinelOne, 2024)
4. **Insecure Interfaces and APIs**: Vulnerabilities in the software or source code that allow outside attackers to exploit and use the resources and services in the cloud. (SentinelOne, 2024)
5. **Denial of Service (DoS) Attacks**: Attacks that overload cloud services using floods of packets and then making the cloud unavailable and unusable to real users. (SentinelOne, 2024)
6. **Advanced Persistent Threats (APTs)**: Prolonged cyberattacks made in such a way that it can infiltrate and steal data from cloud environments over time. (David Puzas, 2024)
7. **Data Loss**: Accidental deletion, hardware failure, or natural disasters along with the lack of backups of data, resulting in the permanent loss of data. (SentinelOne, 2024)
8. **Malware Injection**: Malware scripts or codes injected into cloud services that can steal data and gain control. (Wayne Jansen, 2011)
9. **Lateral Movement Attacks**: Attackers move within the network and escalate privileges to gain access to the resources in the cloud. (Wayne Jansen, 2011)

 doi:10.20944/preprints202501.0745.v1

10. **Configuration Vulnerabilities**: Weak or misconfigured settings that make cloud services vulnerable to outside networks and makes the data or services exploitable by unauthorized individuals. (David Puzas, 2024)
11. **Inadequate Identity, Credential, and Access Management**: Poorly managed IAM settings that creates vulnerabilities, allowing unauthorised users to access sensitive resources and use or steal the data in the cloud. (David Puzas, 2024)
12. **Lack of Cloud Security Policy**: lack of policies and regulations can cause improper practices and management of the cloud system and that can lead to gaps in security. (David Puzas, 2024)
13. **Weak Encryption and Key Management**: improper management of encryption keys could allow unauthorised users to access and steal the sensitive data within the cloud. (Wayne Jansen, 2011)
14. **Insufficient Compliance Controls**: being unable to follow industry standards and regulatory rules can make cloud systems vulnerable to newer exploits which can result in data breaches and legal issues. (David Puzas, 2024)
15. **Inadequate Logging and Monitoring**: not being able to detect unauthorised activity or attacks because of the lack of monitoring or skilled individuals for it. (Wayne Jansen, 2011)
16. **BYOD (Bring Your Own Device) Security Risks**: Devices connecting to the cloud without proper security measures can cause the increase of exposure to outside threats and also makes the cloud more vulnerable to attacks like DDoS. (Wayne Jansen, 2011)
17. **External Threats**: cyber threats like hacking, phishing, or ransomware from external elements. (David Puzas, 2024)
18. **Insecure Data Transfer**: not transferring data in a secure way that lacks proper encryptions or poor network security can cause theft or alteration of the data by outside elements. (SentinelOne, 2024)
19. **Application Vulnerabilities**: Bugs and vulnerabilities in the application layer that makes the application exploitable can be exploited by outside users. (Wayne Jansen, 2011)
20. **Lack of Physical Security for Data Centers**: Unauthorised physical access to data centres or server devices that store cloud data can make it possible to cause harm physically. (Wayne Jansen, 2011)
21. **Cross-tenant Data Access**: In a multi-tenant cloud environment where the environment is shared between the users, if one user gains unauthorised access to another user's data it can lead to hacking. (SentinelOne, 2024)
22. **Vulnerability of Virtual Machines (VMs)**: exploitable variables in the systems of the VMs can make it possible for attackers to exploit the VMs itself and access cloud resources.
23. **Shadow IT**: Unmonitored cloud applications and resources that are being used or illegally used without authorisation and the knowledge of IT management can increase risk by making the cloud more vulnerable from outside individuals. (David Puzas, 2024)
24. **Supply Chain Attacks**: Vulnerabilities from third-party softwares or services which can be legal or illegal can mix up into the cloud environment making it vulnerable from outside. (SentinelOne, 2024)
25. **Resource Exploitation**: Unauthorised use of cloud resources can lead to increased costs and security risks that can be exploited. (Wayne Jansen, 2011)
26. **Lack of regular updates**: Lack of regular updates of cloud software can make it vulnerable to newer threats as newer exploits are usually undetectable and unpreventable by older technologies and softwares. (Wayne Jansen, 2011)
27. **Lack of regular testing**: Lack of regular penetration testing can make the cloud vulnerable as management does not get aware of new threats and exploits to the older software. (Wayne Jansen, 2011)
28. **Lack of security systems**: Lack of properly updated firewalls and IDS can make the cloud highly vulnerable to newer outside threats. (David Puzas, 2024)

 doi:10.20944/preprints202501.0745.v1

2.4. Example Security-Related Technology

Cloud computing security relies on a combination of technologies and tools to protect cloud environments, data, applications, and services. Key components include:

1. Identity and Access Management (IAM)

IAM is critical for controlling access to cloud resources, managing identities, and preventing unauthorised access. Commonly used technologies include single sign-on (SSO), multi-factor authentication (MFA), role-based access control (RBAC), and attribute-based access control (ABAC). Examples are AWS IAM, Azure Active Directory, and Google Cloud IAM. (TechTarget, 2023; NIST Guidelines, 2023; Nayyar et al., 2021).

2. Data Encryption

Data encryption ensures the confidentiality of data at rest by encoding it and during transmission data is also scrambled making it only comprehensible if decrypted. Symmetric/asymmetric encryption, key management systems (KMS), and secure transport protocols such as TLS are all commonly used. Examples include the AWS Key Management Service (KMS), Azure Key Vault, and Google Cloud Key Management. (Cryptography Academy, 2023; TutorialsPoint, 2023).

3. Network Security and Firewalls

Firewalls inspect network traffic to determine access permissions, securing network and application traffic in the cloud. Technologies include network-based firewalls, Web Application Firewalls (WAF), virtual firewalls, and Firewall-as-a-Service (FWaaS). Notable examples are AWS Network Firewall, Azure Firewall, Google Cloud Firewall, and Cloudflare WAF (Cloud Security Alliance, 2023; AWS Documentation, 2023).

4. Intrusion Detection and Prevention Systems (IDPS)

IDPS solutions monitor cloud environments for threats, policy violations, and unauthorized activities. They utilize classical detection, anomaly detection, and behavior-based analysis, which are frequently combined with SIEM systems. Examples include AWS GuardDuty, Azure ATP, and Google Cloud Intrusion Detection.

5. Endpoint Protection and Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) solutions monitor virtual machines and other cloud endpoints for threats using anti-malware, real-time monitoring, behavioural analysis, and automatic threat quarantine. Examples include CrowdStrike Falcon, Microsoft Defender for Endpoint, and CB Defence. (Carbon Black Cloud) (Endpoint Security Guide, 2023; Gartner Reports, 2023).

6. Data Loss Prevention (DLP)

DLP systems protect sensitive data against unauthorized disclosure and compliance violations by scanning, encrypting, and categorizing it in accordance with regulations. Examples: Google Cloud DLP, Azure DLP, and AWS Macie. (Forrester Research, 2023; Google Cloud Security Blog, 2023).

Examples MPLS security-related technology related to Cloud Computing Security:

Encryption is a critical component of cloud computing security, ensuring the safety of data during storage, processing, and transmission. For example, **data-at-rest encryption** utilizes robust encryption algorithms such as AES-256, with customer-managed keys (CMKs) offering enhanced control over key management, including rotation, revocation, and policy enforcement (TechTarget; TutorialsPoint, 2023)

Similarly, **data-in-transit encryption** ensures secure communication between devices and cloud services, often implemented via Transport Layer Security (TLS) and end-to-end encryption (E2EE), protecting data throughout transmission (Cryptography Academy, 2023; Shah et al., 2022).

In **cloud-based applications**, encryption plays a pivotal role in securing sensitive data at multiple levels. For instance, Software-as-a-Service (SaaS) solutions incorporate file-level and transit encryption by design, while database encryption protects sensitive information at the row or column level, ensuring unauthorized access renders the data unreadable (NIST Archives).

 doi:10.20944/preprints202501.0745.v1

By addressing traditional and cloud-specific threats, encryption helps mitigate vulnerabilities such as side-channel attacks and abuse of cloud services, reinforcing confidentiality, integrity, and access control in cloud environments (TechTarget; Cryptography Academy, 2023).

Need of Encryption – The security threats associated with cloud computing can be broadly categorized as traditional security threats and new threats specific to cloud computing environments (side channel attacks, virtualization vulnerabilities and abuse of cloud services).

Encryption methods for data security in cloud

Encryption is the mechanism of protecting the private data of a user. Public and private keys can be used to achieve encryption of the data, but the effectiveness of the encryption depends on how well the keys are used.

A. RSA Algorithm

RSA, an acronym for Ron Rivest, Adi Shamir, and Leonard Adleman, is a widely used encryption algorithm designed to secure data. It ensures that only authorized users can access encrypted information. The process begins with encrypting user data, which is subsequently stored on the cloud.

The algorithm employs Public and Private keys for decryption. The Public Key is universally known, whereas the Private Key remains exclusive to the data owner. The cloud provider authenticates users and facilitates access to the encrypted data. RSA operates as a block cipher, mapping each message to an integer. Encryption is performed by the cloud service provider, and decryption is carried out by the authorized cloud user. Figure 1 shows RSA algorithm.

Steps Involved in the RSA Algorithm:

1. Select two prime numbers, ppp and qqq.
2. Calculate nnn, where n=p×qn = p \times qn=p×q.
3. Compute Euler's Totient, w(n)=(p−1)×(q−1)w(n) = (p-1) \times (q-1)w(n)=(p−1)×(q−1).
4. Choose an encryption key, eee, such that e<w(n)e < w(n)e<w(n) and GCD(e,w(n))=1\text{GCD}(e, w(n)) = 1GCD(e,w(n))=1.
5. Determine the decryption key, ddd, where d×e≡1mod w(n)d \times e \equiv 1 \mod w(n)d×e≡1modw(n).
6. Encrypt the message, computing cipher text CCC using the formula C=Memod nC = M^e \mod nC=Memodn.
7. Decrypt the cipher text, retrieving the plaintext MMM using the formula M=Cdmod nM = C^d \mod nM=C d mod n.

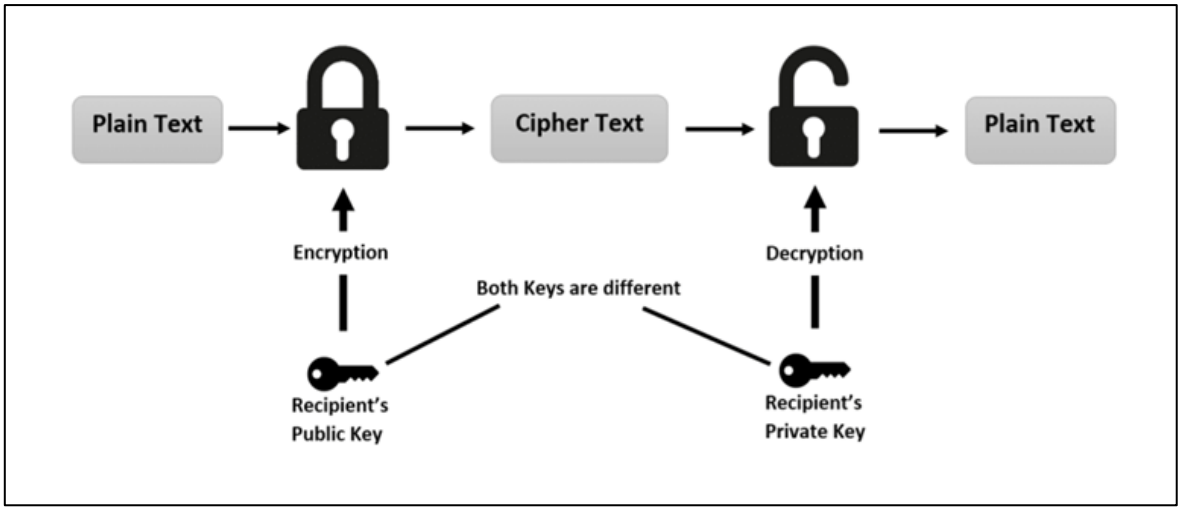

Figure 1. RSA Algorithm.

 doi:10.20944/preprints202501.0745.v1

3.0. DISCUSSION ON THE IMPACT

3.1. Benefits of Cloud Computing Security

Enhanced Data Protection and Compliance

Cloud security frameworks and tools are made to shield private information against breaches, loss, and illegal access. Numerous cloud service providers (CSPs) provide more sophisticated encryption, intrusion detection, and data backup services than the majority of businesses could handle on their own. For instance,organisations can secure data while it's at rest by encrypting it with a program like BitLocker or FileVault. (Sandesh Achar 2022; Sindiramutty, Tan, Shah, et al., 2024). Cloud security measures are frequently in line with regulatory standards like Compliance General Data Protection Regulation (GDPR) Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI-DSS), which impose strict data protection requirements on firms managing sensitive data and ensure their clients' data is protected and that their systems and data are safe from unauthorised access (Sharma et al., 2021). Cloud security lowers the chance of compliance infractions, which can lead to expensive fines and harm to one's reputation, by following these guidelines.

Scalability of Security Solutions

Due to the tremendous scalability of cloud security solutions, enterprises can more easily modify their security resources in response to demand. Cloud security solutions are dynamically scalable to meet growing workloads as companies grow or experience periods of high usage. For companies that deal with varying activity levels, like e-commerce websites during the holidays, scalability is essential. They may guarantee ongoing protection without needing extra physical infrastructure by utilising cloud security (Singhal et al., 2020). Therefore, businesses may scale resources up or down in response to demand with cloud-based security services, ensuring cost-effectiveness and peak performance. While keeping a strong security posture, this scalability enables organisations to meet the changing demands of their operations. (Vinugayathri Chinnasamy,2024; Sindiramutty, Tan, & Wei, 2024)

Cost-Effectiveness and Efficiency

Many businesses work with CSPs for cloud security and with this, businesses could minimise the expenses associated with maintaining their own security infrastructure (Kinza Yasar, 2024). Cloud computing offers significant cost savings on IT-related expenses, such as reduced implementation and maintenance costs and a reduction in the need to buy and maintain hardware and even eliminates the need for skilled IT personnel. This is because cloud providers usually work on a subscription basis, businesses can only pay for the security services they really utilise. Businesses can increase overall operational efficiency by freeing up resources to concentrate on core competencies by assigning security tasks to CSPs.

Improved Disaster Recovery and Business Continuity

Cloud computing promotes faster and more accurate information and application recovery. It is the most productive recovery plan with least downtime. Cloud security systems also offer data redundancy and backup services, contributing in preventing any losses brought on by unforeseen events. Automatic backup processes typically occur in cloud settings, where data is regularly backed up according to set schedules. To help organisations easily backup and recovery critical data in the case of a disaster at their office locations, these backups might include everything from individual files to complete server instances or databases (Kinza Yasar, 2024). Even in the case of cyberattacks, natural disasters, or other disturbances, data is protected by the reliable disaster recovery and backup solutions that cloud providers offer. Data may be swiftly stored and restored using automated

 doi:10.20944/preprints202501.0745.v1

backup solutions, guaranteeing less downtime and promoting business continuity. For example, small and medium-sized businesses (SMEs), who do not have the funds to develop and operate internal disaster recovery systems, can especially benefit from this advantage.

Advanced Threat Detection and Prevention

Cloud security providers often employ the latest security measures and technologies, which improves prevention against cyber attacks. Numerous cloud security companies provide technologies that monitor and identify questionable activity using artificial intelligence and machine learning. Cloud computing security makes it simple to identify attacks through endpoint scanning and global threat intelligence. Additionally, cloud security providers utilise a number of advanced safety features to protect the data and applications of their clients by providing improved protection and constant monitoring (CDNetworks, 2020; Waheed et al., 2024). By automatically reacting to threats, these solutions can help stop breaches before they cause serious harm. AI-driven anomaly detection, for instance, can spot odd login habits or requests for data access, instantly notifying security staff and facilitating a quicker reaction to possible security issues.

3.2. Limitations of Cloud Computing Security

Complex Compliance and Regulatory Challenges

The shared responsibility approach holds companies accountable for specific security measures, even though cloud providers frequently assist with regulatory compliance. This can complicate compliance, particularly for businesses in highly regulated sectors. For instance, failure to adhere to industry standards and regulatory regulations can result in fines, legal repercussions, and harm to one's image. Examples include improperly managing healthcare data in accordance with HIPAA standards or personally identifiable information (PII) in violation of GDPR (CDNetworks, 2020). Furthermore, data residency regulations need that information be kept within specific territorial bounds, which can be challenging to administer in cloud systems because information may be dispersed across several data centres across the globe.

Increased Risk of Data Breaches

Cloud infrastructures are still vulnerable to data breaches even with the robust security protections provided by CSPs. For example, unauthorized access to sensitive customer data, including financial records, intellectual property, and personal information, that is stored in cloud databases.Data breaches can result from human error or negligence, incorrectly setup services, insufficient access safeguards, targeted malicious attacks, cloud application vulnerabilities, and other security policy flaws in threat intelligence, vulnerability mitigation, and threat detection (Vinugayathri Chinnasamy,2024; Wen et al., 2023). Cloud system vulnerabilities have been brought to light by high-profile data breaches, which has strengthened the need for ongoing monitoring, better access control, and comprehensive security audits.

Dependence on Third-Party Providers

Organisations that depend on cloud providers for security are reliant on the dependability, policies, and incident response capabilities of the provider. The organisation's data security may be directly impacted by service outages or security flaws on the provider's end. Therefore, security flaws at these points result in illegal authentication, encryption breaches, and false access controls. These risks are due to weak API credentials, key management errors in the operating system (OS), unpatched software, and hypervisor issues (Abdullah Aljumah, Tariq Ahamed Ahanger, 2020; Alex et al., 2022). In comparison to on-premises security, this reliance restricts an organisation's ability to manage its own security, which could lead to delayed reactions to attacks or incidents.

 doi:10.20944/preprints202501.0745.v1

Limited Customization of Security Controls

Cloud security solutions are frequently standardised to cater to a wide range of users, businesses with particular security needs may have fewer alternatives for customisation. Smaller providers might not have the freedom to customise solutions to meet demands, even while larger CSPs might offer some customisation. Some cloud security services' one-size-fits-all approach may not adequately meet the security needs of organisations with operational or compliance constraints. For example, healthcare organizations must follow strict regulations such as HIPAA or Personal Data Protection Act (PDPA) in Malaysia, which demand specific measures such as advanced access controls, encryption, and detailed audit logs. While cloud providers do offer standard security features, they often fall short of meeting these exact needs. For instance, their logging systems might not record everything the law requires, or their encryption tools might not let organizations manage their own keys. This forces healthcare providers to rely on extra tools or complicated customizations to stay compliant.

3.3. Future Potentials of Cloud Computing Security

Advances in Artificial Intelligence and Machine Learning

By automating threat detection, enhancing incident response, and spotting vulnerabilities before they can be exploited, artificial intelligence (AI) and machine learning have the potential to revolutionise cloud security. Large data sets can be analysed by AI-driven security systems to find trends and react to risks instantly. These technologies may eventually make predictive security measures possible, which would take a more proactive approach to cloud security by anticipating and addressing problems before they materialise. In other words, it's a proactive defence against emerging threats makes it a significant advancement in cloud security as it allows organisations to identify and get rid of dangers before they have a chance to compromise the cloud infrastructure (Kinza Yasar, 2024; Alferidah & Jhanjhi, 2020).

Quantum-Resistant Encryption

Traditional encryption techniques could be at risk from the emergence of quantum computing since these machines can someday crack common cryptographic algorithms. To combat these threats, scientists are creating encryption methods that are immune to quantum technology. Cloud providers are getting ready for the future by implementing quantum-resistant encryption into place to protect data from any risks posed by quantum computing. While Google Cloud and Microsoft Azure are experimenting with more complex algorithms, International Business Machines Corporation (IBM) is already utilising lattice-based cryptography in its services. The goal of these initiatives is to keep systems safe as technology develops by protecting sensitive data, guaranteeing secure data transfer, and safeguarding vital applications like banking, healthcare, and the Internet of Things (IoT). To keep cloud settings safe even as technology develops, cloud providers are probably going to include quantum-resistant algorithms in their security packages.

Expansion of Zero-Trust Architecture

The use of Zero-Trust Architecture (ZTA) to secure cloud environments is growing in popularity. Unauthorised access and lateral movement within a network are reduced by Zero-Trust, which treats each access request as a possible threat. With zero trust, a user's identity or network location does not automatically provide them access to resources, data, or rights. Instead, regardless of whether an access request comes from inside or outside the network boundary, it is thoroughly authenticated, authorised, and monitored. Cloud providers will probably incorporate more Zero-Trust principles into their offerings as ZTA technology develops, adding an extra degree of security for private information and apps. By implementing zero-trust policies, organisations can reduce the impact of any breaches and the danger of lateral movement attacks. Zero-trust models should become

 doi:10.20944/preprints202501.0745.v1

more common in the context of cloud network security as more organisations utilise cloud-based architectures and distributed workforces (Kinza Yasar, 2024; Alkinani et al., 2021).

Increased Use of Blockchain for Data Security

Cloud security may benefit from blockchain technology's decentralised and impenetrable approach to data management. Blockchain can improve data integrity, auditability, and access control security by logging transactions on a distributed ledger. The integration of blockchain technology with cloud computing has strengthened security across sectors such as banking, healthcare, and IoT. Innovations include frameworks utilizing SHA-256 Cryptographic Hash Algorithm, Elliptic Curve Integrated Encryption Scheme (ECIES) encryption, and blockchain-enabled scheduling to boost data protection, authentication, and resource distribution. Blockchain fosters trust, prevents data tampering, and eliminates the need for third-party intermediaries through smart contracts (Humayun et al. ,2020). However, challenges like latency, scalability, and computational overhead persist. Future efforts aim to tackle real-world implementation constraints, address vulnerabilities like DoS/DDoS attacks, and enhance data privacy while improving cost-efficiency and system performance (Bader Alouffi, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, Muhammad Ayaz, 2021; Babbar et al., 2021). Blockchain may be utilised in the future to provide more transparent and safe records of data access and modifications, giving businesses an unchangeable record of every action made on their data in cloud environments.

4.0. DISCUSSION ON SECURITY COUNTERMEASURES

4.1. Security Countermeasures

The rapid popularity of cloud computing is also accompanied by increasing complexity in the security landscape. Organisations must deploy rigid security measures so that sensitive data and key infrastructure can be protected. This section will review major security measures that may be employed to reduce the dangers linked to cloud computing. By understanding and implementing these tactics, the organisations will be protecting their assets.

Countermeasures for DDoS Attacks

According to (Kafhali et al., 2021; Figure 2) most prevalent existing countermeasures are DDoS prevention techniques in the Cloud like signature-based, anomaly-based and hybrid methods of detection. These methods classify how traffic should be normal or malicious by monitoring it precisely. Source-end, access point, intermediate network and distributed defences: their deployment strategies allow them to efficiently filter malicious traffic. CIDS or Collaborative Intrusion Detection Systems exchanged information over the region to find regular suspicious activity. Other safeguards include firewalls, rate-limiting, and Intrusion detection (to catch threats in their early stage). This enables the source of an attack to be localised quickly using traceback techniques and IP spoofing detection.

 doi:10.20944/preprints202501.0745.v1

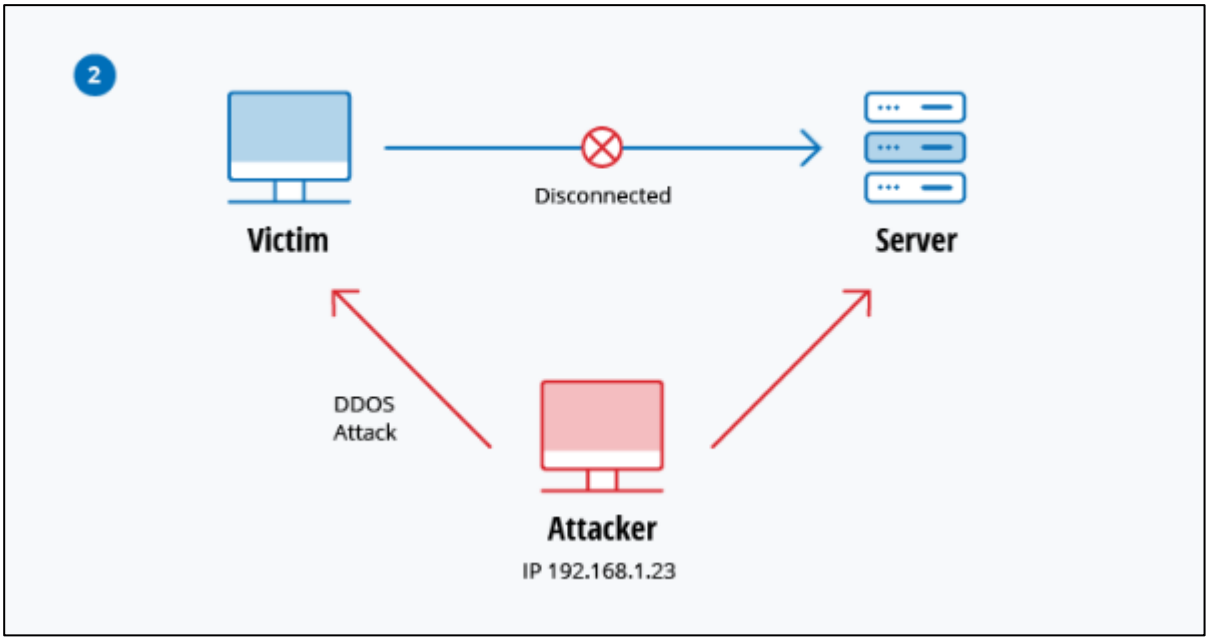

Figure 2. DDoS Attack Illustration (Netwrix Blog).

Countermeasures for Data Breaches

To safeguard against data breaches in cloud computing, organizations must prioritize robust access controls. Strong password policies, multi-factor authentication, and role-based access controls can significantly mitigate unauthorised access. Regular security audits and vulnerability assessments are essential to identify and address potential weaknesses (Sushmith, 2024; Fortinet, n.d.).

Encryption is a powerful tool for protecting sensitive data both at rest and in transit. Additionally, implementing a comprehensive data loss prevention (DLP) solution can help prevent accidental or malicious data leaks. Regular security awareness training for employees is crucial to reduce the risk of human error. By educating employees about security best practices, organisations can minimize the likelihood of successful social engineering attacks. Staying up-to-date with the latest security best practices and industry standards, such as those provided by NIST and CISA, is essential for strengthening cloud security posture (Balbix, 2024; America's Cyber Defense Agency, n.d; Brohi et al., 2020).

 doi:10.20944/preprints202501.0745.v1

4.2. Proposed Countermeasures (Defense Solution)

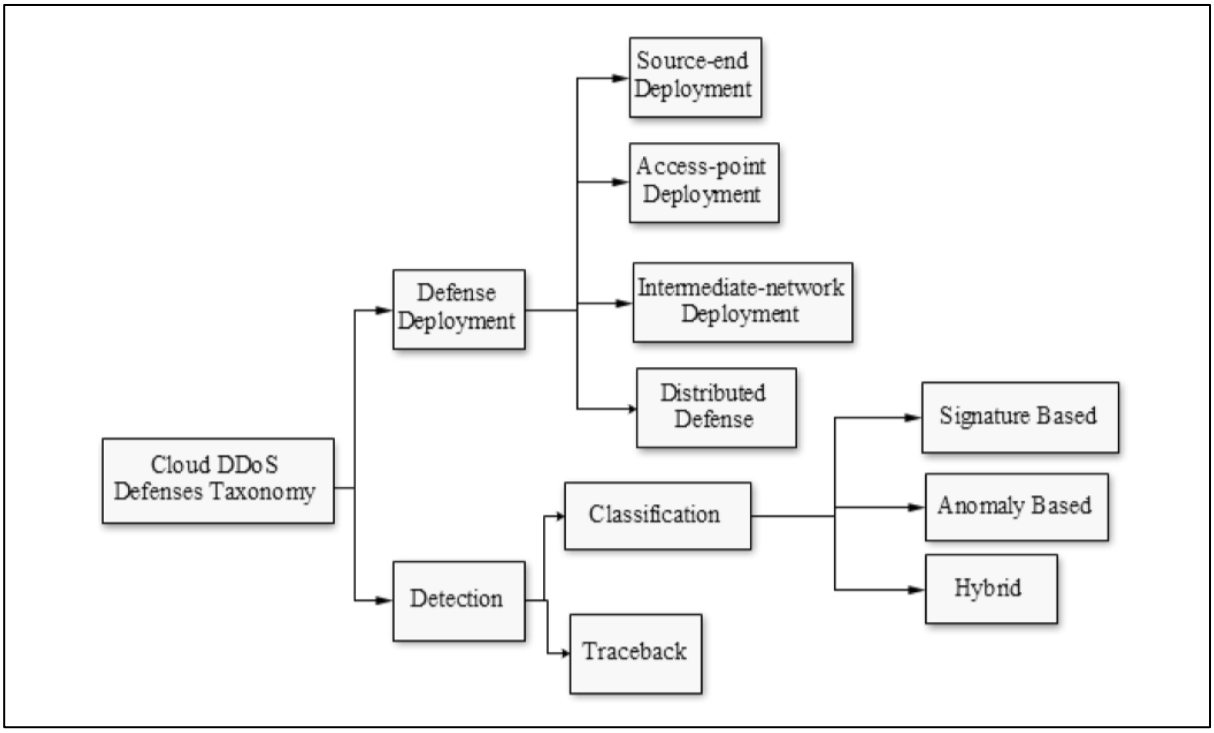

Figure 3. Cloud DDoS Defense Taxonomy (Kafhali et al., 2021).

Proposed Countermeasures Cloud DDos attack (Defense Solution)

Advanced DDoS defence involves hybrid Intrusion Detection Systems (IDS) combining anomaly-based and signature-based detection for precision and reduced false positives (Kafhali et al., 2021; Figure 3). These work together with SOA-based traceback and cloud filters to identify spoofed IPs reducing the impact of attacks. Distributed defence combines source-end, access point, and intermediate solutions resulting in layered protection. This classification of cloud DDoS defences (shown in the figure) provides a systematic way to mitigate service interruptions through security against advanced threats Chesti et al., 2020. Revised IDS work like Cloud Security Break-in Alarms and the firewalls with traffic inspection and source rate limiting block such traffic i.e. stop bandwidth exhaustion by sending malicious traffic. These measures combine to provide robust protection with little pullback in service ("View of A Survey on Cloud Computing Security Threats, Attacks and Countermeasures: A Review," n.d.).

Comments:

The countermeasures provide robust protection, combining hybrid IDS, distributed defence, and traceback methods to detect and mitigate attacks effectively. However, constant updates, resource optimization, and seamless integration are essential for maintaining accuracy and minimising false positives, ensuring scalability and efficiency against evolving threats.

Proposed Countermeasures Data Breach Attack

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 January 2025 doi:10.20944/preprints202501.0745.v1

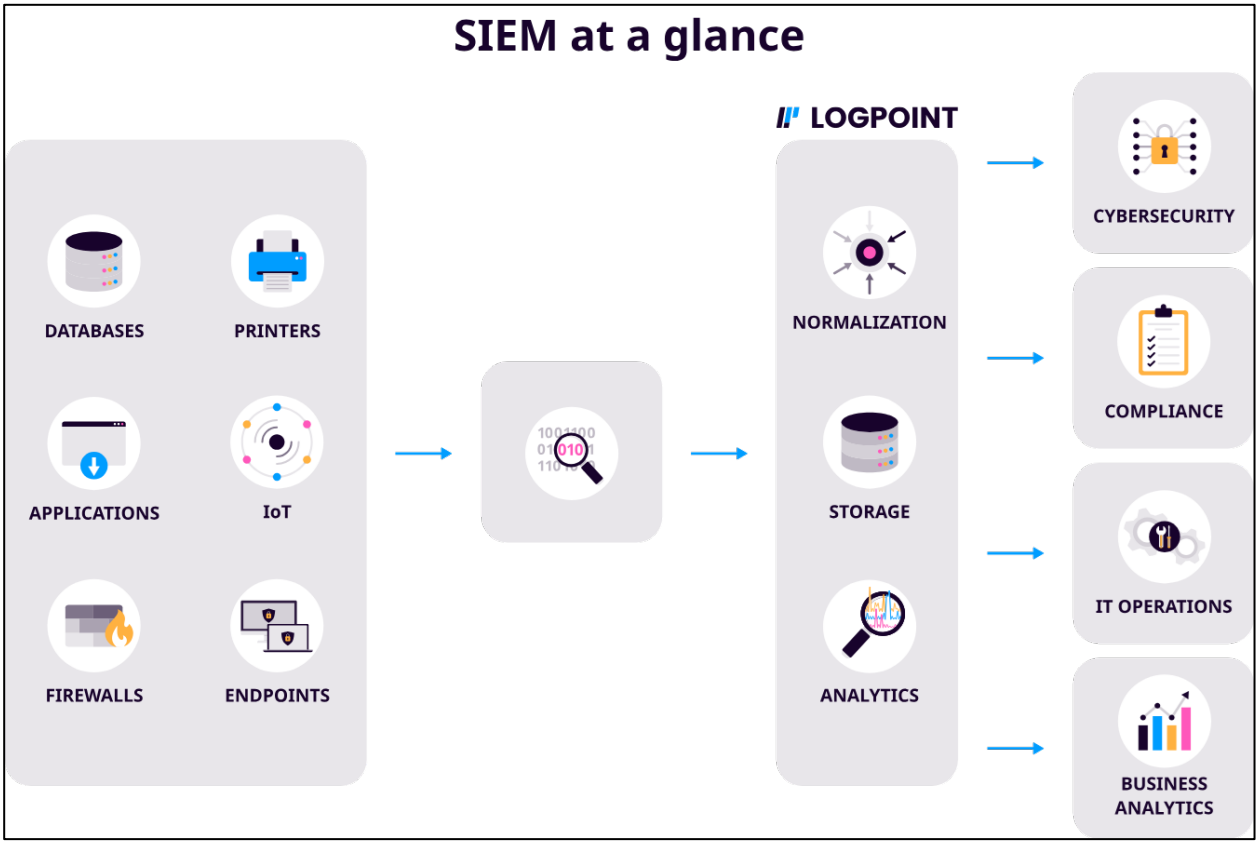

Figure 4. What is SIEM? A complete beginner guide to SIEM and Logpoint (Dalgaard, 2024).

According to (Dalgaard, 2024; Figure 4) to bolster security against data breaches in cloud computing, a comprehensive Security Information and Event Management (SIEM) system is indispensable. SIEM solutions consolidate security logs, enabling real-time threat detection and response. By analysing log data for anomalies, SIEM systems can identify potential breaches early, allowing for swift mitigation.

According to (Gupta, 2023 ; Figure 5), another vital defence is a Cloud Access Security Broker (CASB). CASBs act as a security layer between users and cloud applications, enforcing policies and monitoring user activity. By controlling access to sensitive data and applications, CASBs prevent unauthorised access and data leakage.

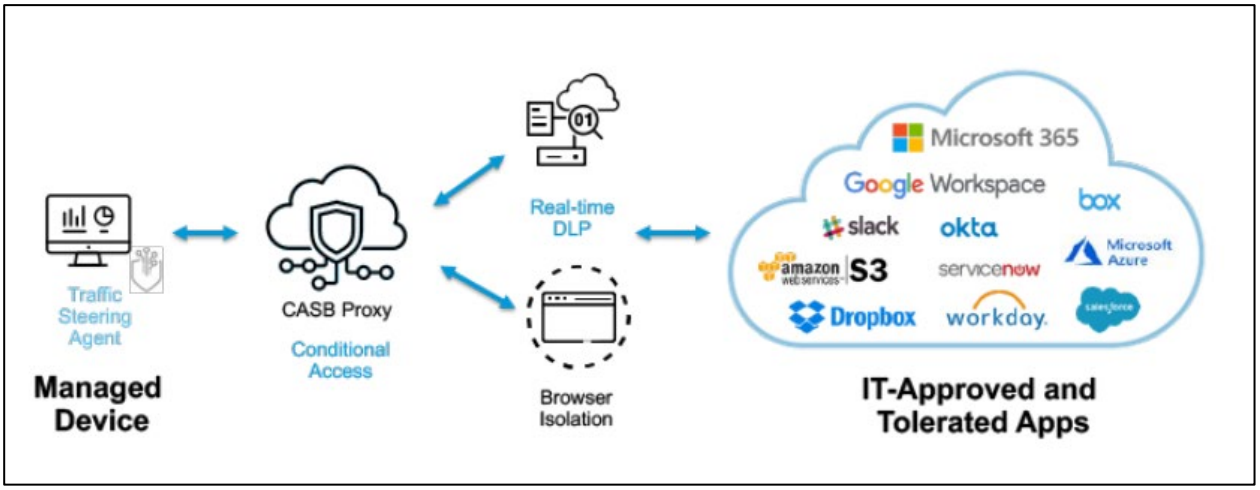

Figure 5. What is Cloud Access Security Broker (CASB)? (Gupta, 2023).

 doi:10.20944/preprints202501.0745.v1

Proposed Countermeasure (IDS)

To enhance cloud security, intrusion detection is a collection of advanced technologies that identifies unwanted actions. Numerous solutions have been created and implemented to protect apps, data, and cloud environments from threats such firewalls and anti-virus, but they still need to be improved. (Chiba et al., 2016) Intrusion Detection Systems (IDS) have changed dramatically over the years, responding to the ever-changing threat scenario. Traditional signature-based IDSs depended on established patterns to recognize known threats. While successful against known threats, some systems struggled to identify unexpected assaults. (Fouda, Ksantini and Elmedany, 2022) Over the various years, multiple approaches have been presented and evaluated using multiple datasets as can be demonstrated from Figure 6, These techniques include, Machine Learning-Based IDS with anomaly detection or behaviour detection and Deep Learning Based IDS with neural network or Natural Language Processing. From the research done by Attou, H, it is obvious that reliable IDS techniques are obtained utilizing ML and DL algorithms (Attou et al., 2023).

Contribution	Year	Methods	Data	ACC (%)
[13]	2016	ANN	-	-
[14]	2022	Gradient Boosting DT	NSL-KDD Bot-IoT IoT 23	100 100 100
[36]	2021	ANN KNN DT SVM NB RF	ISOT-CID	92 100 100 81 60 100
[38]	2018	LSTM	NSL-KDD	98.94
[39]	2022	RF, NB, SVM, KNN	-	92
[40]	2020	SVM	-	96.23
[41]	2021	RF, KNN, NB	-	99.76
[42]	2021	Ensemble Learning	CICIDS 2017, CloudSim	97.24
[45]	2022	RF, GA	NSL-KDD UNSW-NB15	92 96
[43]	2019	RF, GBM, Adaboost	NSL-KDD	99.5
[46]	2020	DT, J48	OneM2Mdata	92
[47]	2021	CNN	Bot-IoT	-
[44]	2022	Ensemble learning	Bot-IoT wustl_IIoT_2021	99.99 99.12
[48]	2023	RF	NSL-KDD Bot-IoT	98.3 100
[49]	2021	LSTM	KDDCup'99 NSD-KDD DARPA KDD CSE-CIC-IDS2018	99.05

Figure 6. A comparison study of several IDSs (Attou et al., 2023).

Therefore what we proposed is a deep learning-based model by leveraging advanced convolutional neural networks (CNNs)-based model architecture integrated with Recurrent Neural Networks (RNNs) In recent years, deep learning-based detection systems have attracted increased attention due to their capacity to perform better with large-scale and complicated network traffic and their ability to learn representations of features from raw data, making them flexible to diverse assault situations. (Liu and Lang, 2019) A CNN model on its own can effectively manage common issues such as data imbalance and feature redundancy, leading to improved robustness and reliability. Furthermore, By using the Pearson correlation coefficient matrix heatmap, relevant features were selected to reduce computational overhead and time complexity while enhancing the precision of the

 doi:10.20944/preprints202501.0745.v1

model. When the model was tested using the CES-CICIDS2018 dataset, it had an accuracy of 98.67% as can be shown in Figure 7. (Aljuaid and Alshamrani, 2024)

When handling sequential data like text or time series, specific architectures are required to comprehend the connections within the sequence. While traditional feed-forward networks struggle with this processing, Recurrent Neural Network (RNN) are suitable for capturing these relationships and can effectively analyze and process sequential data with long-term dependency. (Beltozar-Clemente et al., 2024) RNN has been used multiple times in tests such as in an article by Nasrullah Khan in June 2024 where a hybrid RNN-RF model was used and produced results that were as close to 99.99% accurate (Khan et al., 2024; Dogra et al., 2021). By integrating the strengths of both CNN and RNN, we were confident that it could effectively process sequential data with spatial elements, potentially resulting in improved detection rates and accuracy, particularly for intricate attack vectors that necessitate sequential data evaluation.

Table 21. Comparison of the latest research on DL for IDSs based on the CES-CICIDS2018 dataset.

Reference	Year	Learning Algorithm	Accuracy
[15]	2020	DNN	95%
[33]	2020	Fully Connected Dense DNN	90%
[34]	2021	Autoencoder	95.79%
[35]	2023	MLP with BP	98.41%
[36]	2022	PCA-DNN	97.77%
[37]	2022	CNN	98.15%
Proposed	2024	Multi-Blocks of CNN	98.67%

Figure 7. Comparison of the latest research on DL for IDSs based on the CES-CICIDS2018 dataset *(Aljuaid and Alshamrani, 2024).*

5.0. CONCLUSIONS

Importance of cloud security for cybersecurity: It can protect data, applications, and services. As organizations adopt cloud infrastructure, the need for effective security grows. Solutions include encryption, data masking, secure storage, and backup technologies to ensure business continuity during disasters. Cloud security provides enhanced data protection, compliance, scalability, cost-effectiveness, improved disaster recovery, and advanced threat detection and prevention. Cloud service providers offer sophisticated encryption, intrusion detection, and data backup services, often in compliance with regulatory standards such as GDPR, HIPAA, and PCI-DSS. This enables enterprises to adjust their security resources to meet growing workloads and maintain operational efficiency. Cloud computing can also facilitate faster and more accurate information and application recovery, reduce downtime, and promote business continuity. Advanced threat detection and prevention technologies such as artificial intelligence and machine learning help prevent cyberattacks and protect customer data and applications.

There are various threats to cloud computing security, such as data breaches, unauthorized access, and cyber threats. Key components include identity and access management (IAM), data encryption, network security, endpoint security, application security, and compliance and monitoring. IAM manages and organizes cloud resource users, while data encryption protects sensitive information. Network security controls data traffic using firewalls, VPNs, intrusion

 doi:10.20944/preprints202501.0745.v1

detection systems, and intrusion prevention systems to protect against unauthorized users and network threats. Endpoint security aims to protect devices connected to cloud services, especially in organizations that adopt a BYOD policy. Application security eliminates vulnerabilities and potential vulnerabilities in cloud applications using web application firewalls (WAFs) and automated vulnerability scanning tools. Compliance and monitoring help confirm compliance with regulatory requirements and track potential threats in the environment. Hardware integration of these components provides a comprehensive cloud security strategy that enhances the overall security posture. However, the best defense architecture requires coordination, regular changes, and compatibility testing.

The growing popularity of cloud computing has led to an increase in the complexity of security measures. To protect sensitive data and critical infrastructure, organizations must implement strict security measures.Firewalls, rate limitation, intrusion detection, and signature-based, anomaly-based, and hybrid detection techniques are some of the defenses against DDoS attacks. Strong password policies, role-based access controls, multi-factor authentication, and access controls are necessary to prevent data breaches. To find and fix possible flaws, regular vulnerability assessments and security audits are crucial. Sensitive information is effectively protected by encryption and deliberate, or unintentional data breaches can be avoided by putting in place a complete data loss prevention (DLP) system. Employees must receive regular security awareness training to reduce the possibility of human mistake. Backtracking techniques, distributed defenses, and hybrid intrusion detection systems (IDS) are suggested defenses against cloud DDoS attacks. A thorough security information and event management (SIEM) system and a cloud access security broker (CASB) are essential for data breaches. Intrusion detection technologies, such as machine learning-based and deep learning-based models, can enhance cloud security by identifying unwanted actions and handling complex network traffic.

References

A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. (2021). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9404177

Academy, C. (2023). *The Data Encryption Standard (DES)*. Retrieved from Cryptography Academy: https://cryptographyacademy.com/des/

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). https://doi.org/10.5281/zenodo.7084251

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

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

Aljuaid, W.H. and Alshamrani, S.S. (2024). A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments. Applied Sciences, [online] 14(13), p.5381. doi:https://doi.org/10.3390/app14135381.

Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185–1191. https://doi.org/10.1049/iet-com.2019.0040

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

America's Cyber Defense Agency. (n.d.). Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cybersecurity-best-practices

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

Attacks from the Cloud. (25 September , 2024). Retrieved from ISC2: https://www.isc2.org/Insights/2024/09/Cloud-Security-INSIGHTS-Attacks-from-the-Cloud#

Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A. and Almusallam, N. (2023). Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing. Applied Sciences, [online] 13(17), p.9588. doi:https://doi.org/10.3390/app13179588.

Aweda, Z. I. (2024, January 3). What is Cloud Computing? Introduction to the Cloud for Beginners. freeCodeCamp.org. https://www.freecodecamp.org/news/what-is-cloud-computing/

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

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

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

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

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

Balbix. (2024, October 21). What is NIST Cybersecurity Framework (CSF) 2.0? https://www.balbix.com/insights/nist-cybersecurity-framework/

Beltozar-Clemente, S., Iparraguirre-Villanueva, O., Félix Pucuhuayla-Revatta, Zapata-Paulini, J. and Cabanillas-Carbonell, M. (2024). Predicting Customer Abandonment in Recurrent Neural Networks using Short-Term Memory. Journal of open innovation, 10(1), pp.100237–100237. doi:https://doi.org/10.1016/j.joitmc.2024.100237.

 doi:10.20944/preprints202501.0745.v1

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

CDNetworks. (2020, December 23). 7 Biggest Cloud Security Benefits. CDNetworks. https://www.cdnetworks.com/blog/cloud-security/what-is-cloud-security-and-what-are-the-benefits/

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

Chiba, Z., Abghour, N., Moussaid, K., omri, A.E. and Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network. Procedia Computer Science, 83, pp.1200–1206. doi:https://doi.org/10.1016/j.procs.2016.04.249.

Chinnasamy, V. (2024, March 4). Understanding cloud security – challenges, best practices and benefits. Indusface. https://www.indusface.com/blog/what-is-cloud-security-and-what-are-the-benefits/

Dalgaard, M. (2024, July 29). What is SIEM? A complete beginners guide to SIEM and Logpoint. Logpoint. https://www.logpoint.com/en/what-is-siem/

David Puzas (2024, April 01). 12 Cloud Security Issues: Risks, Threats, and Challenges. https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-risks/

Davis, L. (2024, November 20). What is cloud computing? The ultimate guide. Forbes Advisor. https://www.forbes.com/advisor/business/what-is-cloud-computing/

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

Fandrick, B. (7 November, 2024). HIPAA vs. PCI DSS requirements for data protection. Retrieved from Liquid Web: https://www.liquidweb.com/blog/hipaa-vs-pci/#:~:text=Data%20protection%20standards%20and%20security%20controls&text=HIPAA%20requires%20covered%20entities%20to,expiration%20dates%2C%20and%20security%20codes.

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

Fortinet. (n.d.). What is a Data Breach and How to Prevent It? | Fortinet. https://www.fortinet.com/resources/cyberglossary/data-breach

Fouda, M., Ksantini, R. and Elmedany, W. (2022). A Novel Intrusion Detection System for Internet of Healthcare Things Based on Deep Subclasses Dispersion Information. IEEE Internet of Things Journal, pp.1–1. doi:https://doi.org/10.1109/jiot.2022.3230694.

GeeksforGeeks. (2020, June 24). Advantages and Disadvantages of cloud security. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-cloud-security/

Gill, S. H., Sheikh, N. A., Rajpar, S., Jhanjhi, N. Z., Ahmad, M., Razzaq, M. A., ... & Jaafar, F. (2021). Extended Forgery Detection Framework for COVID-19 Medical Data Using Convolutional Neural Network. *Computers, Materials & Continua*, *68*(3).

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

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

Gruber, D. & TechTarget, Inc. (2024). Advances in Endpoint Security (By Broadcom). https://docs.broadcom.com/doc/advances-in-endpoint-security

Gupta, P. (2023, March 26). What is Cloud Access Security Broker (CASB)? - Pradeep Gupta - Medium. Medium. https://medium.com/@pradeepgupta_9558/what-is-cloud-access-security-broker-casb-a6bbbf468dd1

Hidayat, T., & Mahardiko, R. (2020). A Systematic Literature Review Method on AES Algorithm for Data Sharing Encryption on Cloud Computing. International Journal of Artificial Intelligence Research, 4(1). https://doi.org/10.29099/ijair.v4i1.154

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

Humayun, M., Jhanjhi, N. Z., Hamid, B., & Ahmed, G. (2020). Emerging smart logistics and transportation using IoT and blockchain. *IEEE Internet of Things Magazine*, *3*(2), 58-62.

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

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

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

Kafhali, S.E., Mir, I.E., Hanini, M., 2021. Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. Archives of Computational Methods in Engineering 29, 223–246. https://doi.org/10.1007/s11831-021-09573-y

Khan, N., Mohmand, M.I., Rehman, S. ur, Ullah, Z., Khan, Z. and Wadii Boulila (2024). Advancements in intrusion detection: A lightweight hybrid RNN-RF model. PLoS ONE, 19(6), pp.e0299666–e0299666. doi:https://doi.org/10.1371/journal.pone.0299666.

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

Li, J., Goh, W., Jhanjhi, N. Z., Isa, F., & Balakrishnan, S. (2021). An empirical study on challenges faced by the elderly in care centres. *EAI Endorsed Transactions on Pervasive Health and Technology*, *7*(28).

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

 doi:10.20944/preprints202501.0745.v1

Liu, H. and Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences, [online] 9(20), p.4396. doi:https://doi.org/10.3390/app9204396.

Maine Basan. (May 28, 2024). Top Cloud Security Issues: Threats, Risks, Challenges & Solutions. https://www.esecurityplanet.com/cloud/cloud-security-threats/

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

Media, T. (23 February, 2023). Why the Cloud is Potentially Vulnerable. Retrieved from ThriveDX: https://thrivedx.com/resources/blog/why-the-cloud-is-potentially-vulnerable#:~:text=Lack%20of%20Physical%20Control,-Cloud%20data%20and&text=There%20is%20limited%20control%20over,is%20so%20vulnerable%20to%20cybercriminals.

Mohammed, I.A. (2019) (PDF) Cloud Identity and Access Management - A Model Proposal, CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL. Available at: https://www.researchgate.net/publication/353887567_CLOUD_IDENTITY_AND_ACCESS_MANAGEMENT_-_A_MODEL_PROPOSA

Muzafar, S. (2021). Energy harvesting models and techniques for green IoT: A review. *Role of IoT in Green Energy Systems*, 117-143.

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

Ot, A. (2023, July 11). The Ultimate guide to cloud Computing. Datamation. https://www.datamation.com/cloud/what-is-cloud-computing/

Pramanik, S., Samantha, D., M, V., & Guha, A. (2022). Cyber security and network security. In Wiley eBooks. https://doi.org/10.1002/9781119812555

Ranger, S. (2022, February 25). What is cloud computing? Everything you need to know about the cloud explained. ZDNET. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/

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

Richman, A. (9 October, 2023). Data Masking vs Encryption: What You Need to Know. Retrieved from K2View: https://www.k2view.com/blog/data-masking-vs-encryption

Saleh, M., Jhanjhi, N., & Abdullah, A. (2020, February). Fatima-tuz-Zahra,''Proposing a privacy protection model in case of civilian drone,''. In *Proc. 22nd Int. Conf. Adv. Commun. Technol.(ICACT)* (pp. 596-602).

Sama, N. U., Zen, K., Humayun, M., Jhanjhi, N. Z., & Rahman, A. U. (2022). Security in wireless body sensor network: A multivocal literature study. *Applied System Innovation*, *5*(4), 79.

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

SentinelOne (2024, October 25). 17 Security Risks of Cloud Computing in 2024. https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/

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

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

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

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

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

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

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

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

Singh Solanki, P., Singh, A., Sao, S., & Atkekar, N. D. (2024). Int. J. of Sci. Research in Network Security and Communication (Vol. 12). Prof. (Dr.) Umesh Kumar Singh. https://doi.org/10.26438/ijsrnsc

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

Srinivasan, K., Garg, L., Chen, B. Y., Alaboudi, A. A., Jhanjhi, N. Z., Chang, C. T., ... & Deepa, N. (2021). Expert System for Stable Power Generation Prediction in Microbial Fuel Cell. *Intelligent Automation & Soft Computing*, *30*(1).

Sushmith. (2024, October 21). Data breaches in cloud computing | Tips to Prevent. Sprintzeal.com. https://www.sprintzeal.com/blog/data-breaches-in-cloud-computing

View of A Survey on Cloud Computing Security Threats, Attacks and Countermeasures: A Review [WWW Document], n.d. URL https://www.milestoneresearch.in/JOURNALS/index.php/IJHCI/article/view/34/46

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

Wayne Jansen, Timothy Grance (2011, Dec), National Institute of Standards and Technology, US. Guidelines on Security and Privacy in Public Cloud Computing. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

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

What are the benefirs of Cloud Computing. (May28, 2024). Retrieved from prosimo.io: https://prosimo.io/what-are-the-benefits-of-cloud-computing/

What are the Benefits of Cloud Security? (2021, August 25). Utimaco. https://utimaco.com/service/knowledge-base/cloud-security/what-are-benefits-cloud-security

What is Cloud Backup? How It Works, Benefits and Best Practices. (5 February, 2024). Retrieved from Spanning: https://www.spanning.com/blog/cloud-backup/

Why is the cloud so cost-effective? (4 Febuary, 2023). Retrieved from Box Blogs: https://blog.box.com/why-is-the-cloud-so-cost-effective

Yasar, K., Froehlich, A., & Shea, S. (2024, June 13). cloud security. Search Security. https://www.techtarget.com/searchsecurity/definition/cloud-security