Article

Not peer-reviewed version

Building Trust in Cloud Computing:Strategies for Resilient Security

Ang Ting Xun , Lim Alan Zhe En , Lim Tze Shen , Ang Ning Xin , Wong Hee Soon , Wong Zi Jun , Harish Ramachandra , Guo Xinghao , Nyi Min Khant , Feng Weitao , Siva Raja Sindiramutty *

Posted Date: 10 January 2025

doi: 10.20944/preprints202501.0716.v1

Keywords: Cloud Computing Security; AI-Driven Threat Detection; Zero-Trust Architecture; Blockchain Security; Adaptive Multi-Factor Authentication

Article

Building Trust in Cloud Computing: Strategies for Resilient Security

Ang Ting Xun, Lim Alan Zhe En, Lim Tze Shen, Ang Ning Xin, Wong Hee Soon, Wong Zi Jun, Harish Ramachandra, Guo Xinghao, Nyi Min Khant, Feng Weitao and Siva Raja Sindiramutty *

Taylor's University, Malaysia

* Correspondence: magan.shiva91@gmail.com

Abstract: Cloud computing is a technology that will change how data is stored, managed, and accessed. It reduces the need for users to set up hardware and computing resources on demand, and it eases things for businesses and individuals, but as cloud computing becomes more common, security problems are becoming a big issue for its future growth. They focus on the three basic models of cloud computing: Software as a Service-SaaS, Platform as a Service-PaaS, and Infrastructure as a Service-IaaS; add the main architectural models: public, private, hybrid, and multi-cloud, analyse their advantages and disadvantages, as well as potential security risks. The cloud computing security system is a most crucial aspect. It includes how technologies such as identity and access management, firewalls, intrusion detection systems, data encryption, etc., protect data and examines the possibility of using new technologies such as artificial intelligence, blockchain, and zero-trust architectures. It should greatly improve the security of cloud computing, using intelligence in threat detection, decentralised management, and ongoing verification. Some common issues are dealt with, including data leakage, unsafe APIs, and insider threats. The importance of focusing on multi-layer defence is then highlighted. We look at the current state of cloud security technologies and strategies, along with future improvements we need. The goal is for cloud service providers and users to work together in using a layered security approach, a shared responsibility model, and new technologies to create a safe and dependable cloud environment. This security model will be able to cope not only with the complexity of network threats but also with the continuity of cloud computing technological development, thereby carrying important values in references for the research and practice of related technologies.

Keywords: cloud computing security; AI-driven threat detection; zero-trust architecture; blockchain security; adaptive multi-factor authentication

1. Background

Cloud Computing is a network of resources hosted online that are used by individuals and companies instead of hosted on a local server or computer. There are 3 main models and 4 development patterns in Cloud Computing that are used, the main models being Software as A Service (SaaS), Platform As A Service (PaaS), and Infrastructure As A Service (IaaS), and the development patterns being Public Cloud, Private Cloud, Hybrid Cloud, as well as Multi-Cloud. Cloud Computing has transformed the way data is stored, managed, and accessed and made itself integral to the lives of countless companies and individuals (Ananna et al., 2023). Its use will only grow over the years due to its usefulness in work and entertainment and its flexibility and convenience. As such, companies and individuals need to focus on security technologies related to Cloud Computing and improve it over time.

Over the years there have been many security-related technologies developed for use in Cloud Computing. In this background, we will briefly discuss Identity and Access Management (IAM), Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). IAM is a set of

 doi:10.20944/preprints202501.0716.v1

important tools that control user identities in the workplace and manage their access to the different resources that they have access to. A few examples of IAM are Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC).

SSO streamlines user access by granting system users access to multiple systems or applications after logging in only one time. This helps to reduce password fatigue in employees or individuals who use SSO because they do not need to remember multiple passwords for multiple accounts. An example of SSO is Google which allows users to access multiple cloud-based systems and applications through one account. MFA creates a more secure environment by requiring multiple forms of authentication to verify a user before letting them access a system or website (Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023). An example of MFA would be a website that requires users to type in a password and after the password has been verified, the user will be sent a one-time authentication code through their email or a text message that needs to be typed in to gain full access. There can also be other authentication factors involved such as biometrics like fingerprints or a smart card (IMI, 2024). RBAC grants permissions to users based on their role in the company. For example, the access, reading, writing and sharing of files can be determined by the role an employee has. It applies to other sectors of a job too, like finances as only employees with the right role can make transactions www.okta.com (2024).

Secondly, are Firewalls. Firewalls are network security devices that are designed to monitor and filter through incoming and outgoing network traffic based on preset rules to prevent unauthorised access to resources and applications. There are also Next-Generation Firewalls that have all the functionalities of regular firewalls but also have additional features such as Packet Filtering to inspect individual packets of data to block malicious ones, Stateful Inspection to make sure that packets are part of legitimate networks, and VPN Awareness so that they can identify encrypted traffic from Virtual Private Networks (VPN) and allow it (Cloudflare, 2024).

Third, are Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS). Intrusion Detection Systems and Intrusion Prevention Systems are systems that monitor the traffic of a cloud's network for malicious activity. An IDS does not take any active steps to halt that malicious activity if detected, it merely alerts administrators and security teams. An IPS however, is a more advanced version of an IDS that actively prevents threats and malicious activity by blocking malicious traffic, terminating malicious content, or adjusting firewall rules to prevent threats (Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023). Both systems share some threat detection methods, such as Signature-Based Detection which is done by analysing network packets for unique characteristics that only appear in malware and Anomaly-Based Detection which is done by using Artificial Intelligence and Machine Learning to create and refine a model of regular network activity over time to use as a baseline. The systems then compare ongoing network activity to the baseline model and respond when deviations occur. (IBM, 2023).

If security is not well maintained or upgraded when it comes to Cloud Computing, the consequences can be devastating. Unfortunately, many companies do not prioritise security for their Cloud Computing. A recent report showed that in 2022, 92% of companies faced security incidents related to APIs which are a core component of Cloud Computing (Keary, 2023). Another consequence that could happen if security technology isn't maintained is data breaches. In 2023, 80% of data breaches occurred because of data that was stored in the cloud which made it a vulnerable target (SentinelOne, 2024; Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023). Lastly, there are Distributed Denial of Service (DDoS) attacks which are done by flooding cloud services with traffic. This deluge of traffic overwhelms cloud applications (Mughal et al., 2024) and websites and renders them unusable for some time because the cloud service cannot keep up with the traffic (Basan, 2024). A simple DDoS attack can be prevented by maintaining essential security infrastructure like Firewalls and IPS.

2. Discussions on How Cloud Computing Security Works

 doi:10.20944/preprints202501.0716.v1

2.1. Component

Cloud computing is an infrastructure that allows users to connect to cloud services via the internet and to use networking technologies to share resources across multiple users. The users then only need to pay for what they use, rather than investing lots of money to make and maintain physical servers or storage devices. This allows small organisations to be able to store and share resources amongst their devices with lesser costs. For IaaS, it will provide virtual computing resources over the internet. Components such as Virtual Machines, storage, and networking. The users can have the flexibility to configure and manage their operating systems and applications but are unable to manage the physical infrastructure. Next, PaaS offers a platform which allows the developer to build, run, and manage the application only. It provides an environment with tools and services, such as databases, middleware, and development frameworks, to aid in application development. Lastly, SaaS can deliver fully managed applications to users using the web browser. The service provider handles everything, from the infrastructure to the applications, and users only need an internet connection to access it.

Even though this brings much convenience and advantages to people utilising the service, it also has its flaws. For example, the data privacy and security of the data. Hosting data off-premises has always raised a lot of concerns among users about data ownership and compliance with privacy laws. The users that utilise this service may be sceptical about the choice of the company they acquire the service from as data security may be at risk if the cloud security is not managed properly. In addition to that, downtime and dependence on Internet connectivity may also be an issue while utilising cloud services as they are very dependent on Internet connectivity, meaning that any interruptions in the service could impact productivity, cause potential data losses, and restrict access to the service (Konatham et al., 2024). Due to the instability and the unpredictability of data security, different regions have different data protection laws, which can complicate storing sensitive data in global data centres.

Now let's talk about the components of cloud computing security. Cloud computing security itself is the set of policies, and latest technology advancements that are designed to protect any sensitive data present in all the applications, and infrastructure of the cloud computing environments of an organisation. Ensuring that all three contents of the [CIA] confidentiality, integrity, and availability of all of the data stored in the cloud. The security measures (Shah et al,. 2024) can be applied from all parts of the infrastructure, including perspectives from the vendor and the user's point-of-view.

First, Identification and Access Management, also well known as IAM. It is a crucial component for ensuring cloud computing security. It enhances accessibility security as it ensures that only authorised users can access cloud resources. This process involves creating unique identities and roles, assigning roles to proper individuals, and then setting permissions to control the access in the system. Usually, multi-factor authentication (MFA) is often implemented together with the IAM to enforce greater security, making sure that the person who is claiming to be an authorised person who has legitimate access to this role is really who they claim they are. MFA achieves this by requiring users to provide two or more verification factors to gain access. Another example of IAM tools also includes the single sign-on (SSO) feature, allowing users to log in with the same set of credentials to access multiple applications (Zaman et al,. 2023) and (Javed et al,. 2023), and federated identity management, which enables users to access resources across different security domains using the same identity (IMI, 2024).

Firewalls are also a commonly used component in cloud computing security. The role of the firewall is to filter any incoming and outgoing traffic based on the predefined security rules that are set by the organisation. This is used to perform an inspection on the packets that are going in and out of the infrastructure, checking if the data packets contain any common signs of malware, mitigating the risk of infrastructure being vulnerable. Common tools used alongside the firewall are intrusion detection systems (IDS) and intrusion prevention systems (IPS) which are used to detect and block any potential threats which may pose a threat to the system. To a certain extent, Virtual Private

 doi:10.20944/preprints202501.0716.v1

Networks are also used by organisations when lots of sensitive data are being used and transmitted across the network, VPN makes sure that all information that is being transmitted across the channel is impossible to intercept by any unauthorised users. Additionally, network segmentation is also employed to divide the network into smaller, isolated segments, limiting the spread of potential attacks (Dawood et al., 2023; Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023).

Diving in further for the security of data, it aims to focus on protecting the data that is actively being transmitted through the network while also protecting the data at rest. To do this, encryption is one of the crucial techniques that must be used, ensuring that data is unreadable and can be classified as useless to unauthorised users but only making it readable to the authorised receiver. To do this, it uses private and public keys to perform encryption so messages can only be readable by the target receiver by using the private and public key pair. Data masking can also be used to hide sensitive information (Humayun et al,. 2023), replacing it with fictional data that retains the general characteristics of the original data without exposing sensitive details (Khader and Karam, 2023). To further aid in data security, data loss prevention (DLP) tools can be used to help monitor and control the flow of data, preventing unauthorised access and transfer of sensitive information (Domnik, J. and Holland, A., 2024; Hussain et al., 2024). Lastly, it is also highly advisable to perform regular backups periodically so we can decrease the severity of the attack such as any data loss or data corruption.

Antivirus software is also an important component of cloud computing as it aims to detect and remove malware which may pose a significant threat to the devices that are connected to the cloud. For example, we can use the "Endpoint Detection and Response system" to constantly monitor our devices for any indications of suspicious activities on our device. Mobile device management solutions can also be used to enforce better security policies on our devices to mitigate the chances of being vulnerable to attacks. And to take additional precautions for our devices, good habits on keeping on track with the newest patch management would be excellent as it helps us ensure that all devices are using the newest up-to-date security software to ensure that all data contained in the devices can be secured from the unwanted view (Dissanayake et al., 2021; Jun et al., 2024).

Besides online security, cloud providers also focus on physical security measures to protect data centres and the underlying infrastructure. For example, having restricted access to major data points by using passcodes, biometrics, and video surveillance, and also having its audit lot to be able to recheck the history of activities (Gair et al, 2022). In addition to this, backup and disaster recovery models should be properly set up. Multi-regional data replication enables efficient recovery of data during attacks, ensuring the data is protected from physical and online disasters (Cloudsecurityalliance.org, 2024; Manchuri et al., 2024).

2.2. Process

Cloud computing security has many combinations of processes that are important for protecting sensitive data and information in cloud computing. This security framework includes a comprehensive set of methods, technologies, and practices designed to protect the stored data and processes in cloud computing. The cloud environments are shared and most of the time managed by a third-party provider. Security measures are important to focus on the various critical concerns, including data privacy, access control, and regulatory compliance (Dawood, M. et al, 2023). As more organisations transition their operations to cloud computing, it becomes necessary to have reliable security mechanisms. When the organisation shifts to cloud computing it aims to mitigate risks associated with cyber threats, unauthorised access, and potential data breaches (Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. 2021; Ravichandran et al., 2024). Effective cloud security enables both service providers and users to achieve the confidentiality, integrity, and availability of their services, and to have a secure operational framework that supports modern cloud computing.

First, one important process for cloud security will be data protection, for example, encryption in securing data during transmission and storage. By using encryption techniques, even if

 doi:10.20944/preprints202501.0716.v1

unauthorised access occurs, the organisations still have confidence that the data remains unreadable, and they are protected from misuse. Other protective measures, like tokenization and data masking, are also used to protect sensitive information. Tokenization replaces sensitive data elements with unique identifiers or tokens, while data masking obscures some values to minimise their exposures. These two techniques improve data security by reducing the risk of unauthorised access, ensuring that sensitive information remains protected even in the accident of a data breach (Sun, P.J. 2019; Seng et al., 2024).

Access management is another potential process of cloud security. Identity and Access Management known as IAM systems limit access to resources, ensuring that only the authorised users can interact with sensitive data and applications. Implementing Multi-Factor Authentication, and MFA adds a layer of security, making unauthorised access more difficult for them (Josic, D., Basic, M. and Zgrablic, L. 2024; Sindiramutty et al., 2024). Besides, Role-Based Access Control ensures users have access only to the necessary data for their roles. This simplification of access management not only protects sensitive data but also reduces the risk of data exposure by limiting user permissions (Mythili, K. and Rajalakshmi, S. 2022).

Network security measures are also important to protect cloud environments from attacks. Cloud service providers implement advanced and modern firewalls to control network traffic and protect against attacks such as DDoS that might disrupt operations. Furthermore, Intrusion Detection and Prevention Systems, IDPS will continuously monitor the traffic, protect against the potential attacks and allow fast responses to detected threats (Srilatha, D. and Thillaiarasu, N. 2023).

Security of applications in cloud security emphasises safe coding practices throughout the software development lifecycle. Regular security testing helps identify and fix vulnerabilities. The role of APIs in cloud communication, and reliable authentication are important to prevent unauthorised access, to protect information and service continuity (Sun, P.J. 2019; Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024).

Compliance and audits are important for industries which deal with specific regulations, such as healthcare under HIPAA or data privacy under GDPR. For organisations to meet these regulatory requirements, cloud providers may work on certifications and conduct regular audits to tackle potential vulnerabilities. Compliance not only reduces the risk of regulatory violations and financial penalties, but it also helps the stakeholders to trust in the organisation's commitment to data protection (IEEE Digital Privacy 2023; Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024).

For monitoring and threat detection processes, we can have Security Information and Event Management systems that compile and analyse data to initiate threat detection and quick responses. Cloud providers often use AI to enhance their intelligence over threats, detecting and addressing potential threats in real time. This integration of AI improves the overall security of cloud computing, enhancing defence against evolving cyber threats (Rosenberg, M. et al. 2024; Sindiramutty et al., 2024).

Finally, the shared responsibility model in cloud security defines the division of responsibilities between cloud service providers and customers. While providers secure the underlying infrastructure, customers are responsible for securing their data, applications, and access controls. This collaborative model promotes a culture of shared accountability and awareness, allowing organisations to significantly improve their security posture and better protect their cloud-based assets (RiskRecon 2023; Sindiramutty, Tan, Shah, et al., 2024).

In conclusion, the processes of cloud computing security form a multifaceted framework important for protecting sensitive data and maintaining operational integrity in cloud environments. As more organisations transition to the cloud, robust security measures become crucial in addressing the unique challenges associated with third-party managed infrastructures. Key security practices such as data protection through encryption, access control via IAM systems, and network safeguards like firewalls and IDPS—are important for preventing unauthorised access and cyber threats. Adherence to regulatory compliance and regular security audits reinforce trust and minimise legal risks for industries with strict data protection standards. Advanced monitoring and AI-enhanced

 doi:10.20944/preprints202501.0716.v1

threat detection systems further strengthen cloud security, allowing for real-time response to evolving cyber threats. The shared responsibility model in cloud security highlights the need for both cloud providers and users to collaborate, ensuring a resilient defence framework. This approach supports confidentiality, integrity, and availability, empowering organisations to better apply the advantages of cloud computing.

2.3. Threat

Cloud computing is still confronting several security threats caused by its vulnerabilities. Many well-known and common cloud computing threats, such as malware injection, denial of service, account hijacking, data breaches, unsecured interfaces, multi-tenancy, and malevolent insiders, will be briefly explained in this study. A few hazards remain unmentioned in this study, including inadequate access control, Advanced Persistent hazards (APTs), cloud service misuse, and more (Kumar and Goyal, 2019; Sindiramutty, Tan, & Wei, 2024). This study solely does not focus on addressing such concerns, which does not mean they aren't essential.

2.3.1. Malware injection

Malware attacks are a common type of attack and one of the biggest problems for cloud computing. Malware injections, which can serve as SaaS on cloud servers, are executed by running embedded code in cloud services (Ahmad et al., 2021; Waheed et al., 2024), whether it is embedded into software or by executing remote commands onto a computer to access or alter a database or website (Hong et al., 2019). Additionally, the operator's data, which is handled and kept on the cloud, is accessed through Cloud malware injection attacks (CMIAs), a sort of cybercrime particular to cloud computing (Ahanger and Aljumah, 2020). These types of attacks occur because of cloud service providers that are susceptible.

2.3.2. Denial of Service

In a Denial of Service (DoS) or distributed Denial of Service (DDoS) assault, a hacker overwhelms the network with packets that generate unnecessary traffic. This could trigger the intended cloud service to require more system resources than are allotted, which will hinder registered individuals from obtaining their data and apps because of sluggish response times or unavailable cloud resources (Kumar and Goyal, 2019; Wen et al., 2023). Improper programs, a hazardous network protocol, a failing network protection architecture, etc., will all contribute to this hazard (Ahanger and Aljumah, 2020). In addition, the inadequate supply problem of insufficient bandwidth is causing DoS assaults on virtual machines (Parast et al., 2021). To avoid this threat, it is recommended that cloud computing adopt load balancing, robust firewalls, traffic monitoring and filtering, and IPS deployment (Ahmad et al., 2021).

2.3.3. Account or Session Hijacking

Hijacking is the illegal takeover of specific permitted services by unauthorized users. This technique involves an adversary remaining in a TCP/IP conversation to steal a user's credentials, or sessions as well (Parast et al., 2021). Weak credentials and insufficient permission validations are frequently used as reasons for an account or service hijacking, and this threat can be performed from either layer (Parast et al., 2021). As a result, this gives the adversary entrance to the user's assets and enables them to steal, modify, remove or sell the user’s sensitive information and identification (Ahmad et al., 2021). Consequently, the credibility of the business would be damaged, and they might incur significant expenses. There will be legal repercussions for sectors like healthcare that prioritize user data confidentiality. These could be addressed with the use of privacy policies, two-factor authentication, and reliable encryption over the exchange of information while travelling (Díaz de León Guillén, 2020).

 doi:10.20944/preprints202501.0716.v1

2.3.4. multi-tenancy

Multi-tenancy refers to the environment that cloud deployment models deliver, which allows numerous customers to share computing resources like hardware, software, services, or data while maintaining the security and segregation of their data (Ahmad et al., 2021). This operating approach may expose consumers to security issues like information leakage because many different people may be using the same piece of hardware or software simultaneously (Parast et al., 2021). Furthermore, exploitation might have occurred if an attacker had gotten hold of co-located services and hosts (Kumar and Goyal, 2019; Alex et al., 2022). This approach should guarantee the confidentiality and safety of data by offering user separation at the hardware resource and application phases, as well as system scalability and metered consumption (Kumar and Goyal, 2019).

2.3.5. Data breach

In cloud computing, a significant proportion of client data is kept in a cloud environment and is extremely precious. Data breaches pose severe threats to cloud computing because they expose confidential and delicate information to unintentional exposure. Deliberate malevolent assaults, errors by humans, cloud application weaknesses, and inadequacies in security rules in detecting threats and vulnerability minimizing are some of the many reasons for data breaches (Ahanger and Aljumah, 2020). The degree of harm caused by data breaches, which can result in monetary losses, public image damages, and other negative effects, could be evaluated based on the severity of the compromised data (Ahmadi, 2024; Alferidah & Jhanjhi, 2020). Encryption of data, digital signatures and fragmentation redundancy-scattering (FRS) are crucial methods for decreasing risk (Parast et al., 2021). Regulations and procedures for data privacy must be implemented, together with access control regulations to avoid unauthorized users (Ahmad et al., 2021).

2.3.6. Insecure APIs

APIs, virtual machines, and software interfaces play a major role in cloud computing by enabling smooth integration as well as compatibility across various platforms and services (Yanamala et al, 2024; Ahanger and Aljumah, 2020). Security issues like unauthorised authentication, encryption violations, and erroneous access controls will result from insecure APIs and interfaces (Ahanger and Aljumah, 2020; Alkinani et al., 2021). The technical causes of insecure APIs include weak API information, key management problems, operating system issues, unpatched applications, and hypervisor issues (Ahanger and Aljumah, 2020). An API is used to give users a connection to cloud services. To ensure that the content being transmitted is always confidential, CSP should make use of appropriate authorization and authentication protocols in addition to timely patching interfaces (Parast et al., 2021).

2.3.7. Malicious Insider

A malicious insider is an individual who has permitted access to an IT system, whether they are a current or previous worker or a shareholder. They purposefully abused their powers to interfere with the reliability of the system, which might have disastrous consequences because the attacks originate internally. Since they will be regarded as daily access, no alarm will be set off until the attacks occur, thus rendering them difficult to identify and prevent (Ahmad et al., 2021). Malicious insiders may arise as an aftermath of inadequate monitoring, poor management of private entry points, and an absence of cloud guidelines (Ahmad et al., 2021; Babbar et al., 2021).

2.4. Example Security-Related Technology

Cloud computing service providers implement a variety of industry-standard security measures to ensure that data is protected. Many cloud computing services provider offers optional features such as multi-factor authentication (MFA), which ensures that users desire to undergo multiple layers of verification before identity access is granted, the result of reinforcing the security of the login

 doi:10.20944/preprints202501.0716.v1

process and ensuring that only authenticated personnel and devices can access the cloud services (msmbaldwin, 2024; Brohi et al., 2020). Microsoft Entra ID plays an important role within Microsoft as a cloud identity management system that implements strong and enhanced security protocols for Microsoft Azure cloud computing services. Microsoft's verification security measures include the Microsoft Authenticator app, FIDO2 Security Keys, and Voice Key authentication. For example, the Microsoft Authenticator application promotes security by sending users a push notification to approve a sign-in attempt which generates a one-time code on the user's phone, which must be entered into the computer or other devices during login to verify their identity (Justinha, 2024; Chesti et al., 2020). Other than Microsoft Azure, AWS Identity and Access Management (IAM) authentication plays a vital role in supporting users with the ability to apply MFA on their AWS cloud computing account to provide an extra security layer that secures their data resources (Talluri and Teja Makani, 2023).

Data protection is the key security which is highlighted in cloud computing. To safeguard the data, data encryption needs to be applied both during the transmission through the network or being stored. For example, Amazon Web Services (AWS) works as a famous cloud computing service provider, employing robust encryption mechanisms as their security. AWS emphasises the encryption of data rest and provides server-side encryption and client-side encryption to ensure security. For Server-side encryption, AWS provides multiple options, including Amazon S3 managed keys (**SSE-S3),** where data is automatically encrypted using 256-bit **Advanced Encryption Standard (AES-256)** algorithms (Amazon.com, 2024). Other server-side encryption (SSE) options include SSE-KMS and SSE-C, each of which provides a different level of encryption key control. With **SSE-KMS (Server-Side Encryption with AWS Key Management Services)**, AWS KMS automatically generates and manages the encryption keys used to secure data in S3 storage buckets. Besides, **SSE-C (server-side encryption using customer-supplied keys)** provides clients with the ability to complete control over encryption and decryption keys themselves. In this particular model, the user is responsible for managing their keys, and AWS S3 handles the encryption process as objects and uploads them to the destination bucket (Purna et al., n.d.). For Client-side encryption, Users are available have control of the entire encryption process and can manage the encryption keys independently. Before uploading data to the AWS S3 bucket, they encrypt it locally, ensuring that only they have access to the encryption key (Amazon.com, 2024).

To ensure the security of the data in transit on the network, AWS applies AWS Web Application Firewall (AWS WAF) to monitor the HTTP/HTTPS request passing through the Amazon gateway, AWS WAF helps block malicious traffic, such as SQL injection (docs.aws.amazon.com, n.d.). AWS integrated with AWS Shield to cater for the activities of **Distributed Denial of services (DDoS)**, it has a standard version that is automatically complementary to all AWS cloud users and the advanced version will offer enhanced features to encounter professional DDoS attacks. The AWS shield protects AWS resources from DDoS attacks at both the Network Layer (OSI layer 3) and Transport Layer (OSI layer 4) and includes the Application Layer (OSI layer 7) (Routavaara, 2020). AWS Shield detection successfully reduces threats involving attacks directly through the critical system, ensuring the security and consistent availability of the AWS system.

Besides, Microsoft Defender for Azure cloud computing is a cloud-native application protection platform (CNAPP) that proposes to safeguard the cloud computing services applicable to confront various types of threats (Microsoft, n.d; Dogra et al., 2021). Defender for Cloud-enabled cloud services security teams to manage development and operation security across multi-pipeline environments (Microsoft, n.d.). The architecture of the Cloud Defender of cloud computing services (AWS, Azure, Google Cloud) is briefly illustrated in Figure 1.

 doi:10.20944/preprints202501.0716.v1

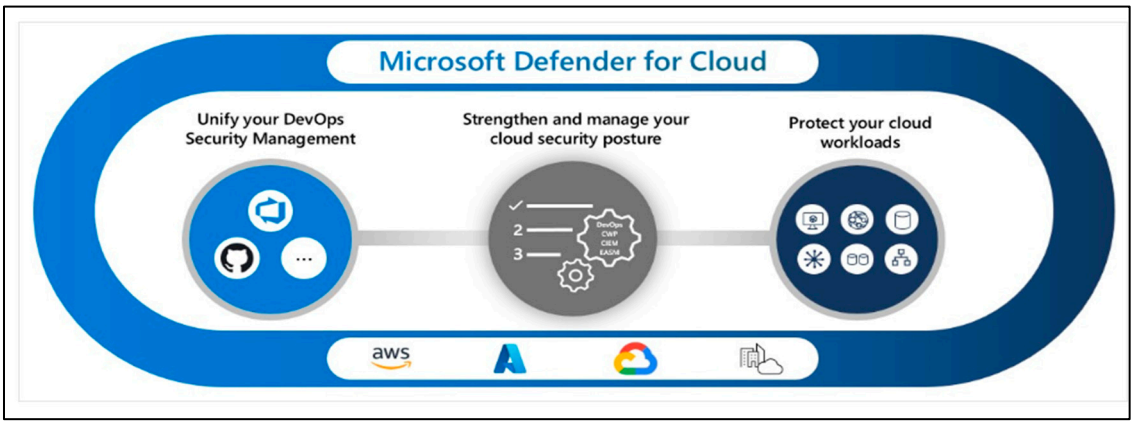

Figure 1. Architecture Overview of Cloud Defender in Cloud Computing (Microsoft, n.d.).

Implementing Threat Detection and Security Monitoring features is essential in cloud computing environments to further improve security. For instance, Amazon GuardDuty can assist in identifying unexpected and potentially unauthorised or malicious activity in users' AWS environment and disclose the potential threats to cloud computing (Moitrayee Chatterjee et al., 2020; Fatima-Tuz-Zahra et al., 2020). In this layer, GuardDuty cooperates with CloudWatch to perform threat detection functions in the cloud environment to provide continuous monitoring of incoming threats (Tan, 2023). AWS GuardDuty offers free foundational threat detection to act on monitoring specific data sources and event logs such as AWS CloudTrail management events, and DNS logs. When upgraded to Use-case focused GuardDuty protection plans, It deployed additional threat detection models from other AWS services including EKS audit logs, RDS login activity, and Amazon S3 data events in CloudTrail (Amazon GuardDuty User Guide Amazon GuardDuty, n.d.). With the example above AWS implements advanced, industry-leading standards in Threat Detection and Security Monitoring within its cloud environment.

3. Discussion on the Impact

3.1. Benefits of Cloud Computing Security

Cloud computing security offers many advantages that organisations can use to better protect data, reduce risks, and improve overall security.

The first major advantage is professional security technical support. Most cloud service providers have dedicated security teams and resources that can monitor security threats in real-time and respond quickly. These service providers usually have deep network security knowledge and technical capabilities and are more capable of responding to security than general organisations (Parast et al., 2021; Gopi et al., 2021). At the same time, advanced automated and intelligent security tools are also considered. The cloud computing environment supports a large number of automated and intelligent security tools that can help detect abnormal activities, block potential threats, and provide timely alerts. For example, automated intrusion detection systems (IDS) and intrusion prevention systems (IPS) can monitor traffic and activities around the clock to quickly identify and respond to threats.

Data redundancy and backup are also one of the major advantages of cloud security. Cloud computing supports multi-regional storage of data and provides highly redundant data backup and disaster recovery options. Through functions such as automatic backup, data mirroring, and cross-regional storage, cloud services can effectively reduce the risk of data loss and ensure rapid data recovery after a security incident (Shirgaonkar et al., 2022; Gouda et al., 2022).

Another major advantage that must be mentioned is the elasticity and scalability of cloud computing platforms, which allow cloud-using companies to easily expand their security resources as security requirements increase. This allows companies to adapt security measures to actual needs

 doi:10.20944/preprints202501.0716.v1

without having to reconfigure extensive hardware or software resources (Abdulsalam & Hedabou, 2021).

3.2. Challenges and Limitations of Cloud Computing Security

Security risks in cloud environments differ in both nature and intensity compared to those in traditional IT setups. In cloud systems, resource pooling enables multiple users to share the same resources via multi-tenancy and virtualization. While these technologies support rapid scalability and efficient resource management, they also introduce certain vulnerabilities.

Multi-tenancy, for instance, can lead to risks associated with data visibility and tracking user operations. On-demand self-service functions, typically managed through web-based interfaces, increase the likelihood of unauthorised access compared to traditional infrastructures. Virtualized environments also present unique risks, such as potential malicious interactions between virtual machines (VMs) and the threat of VM escape. Additionally, the interdependence of cloud service models—where SaaS applications are hosted on PaaS, which itself relies on IaaS—creates a cascade of security dependencies. An attacker gaining control over IaaS could compromise PaaS, leading to potential vulnerabilities in SaaS. Therefore, a security breach at any service model layer can expose other layers to risk (Parast et al., 2021; Humayun et al., 2022).

Private cloud models, being designed for single-organisation use, retain many of the same vulnerabilities found in traditional IT environments. However, public, community and hybrid clouds face cloud-specific risks, primarily due to administrative controls managed by various users and third-party entities. The multi-tenant nature, virtualized resources, and shared file systems pose additional challenges. Effective isolation of multiple tenants and their resources demands an elevated level of security.

In the following sections, we will explore the primary security challenges in cloud computing, categorised into

(a) Communication Challenges

(b) Virtual Network Limitations

Some cloud technologies, such as virtualization, impact multiple service models—affecting both IaaS and PaaS layers simultaneously—rather than any one model specifically.

3.2.1. Communication limitations

There are significant limitations in the communication of cloud computing security, which can affect information exchange between cloud-using organisations, the sharing of threat intelligence, and collaborative processing when responding to security incidents.

The first is the legal and compliance issues of information sharing. In different countries and regions, data privacy laws and data protection regulations, such as GDPR, affect information sharing between cloud service providers and customers, especially when sensitive data or customer privacy is involved. This makes cross-border collaboration more complicated because different laws impose restrictions on data transmission and sharing (Sampson & Chowdhury, 2021; Jhanjhi et al., 2021).

Another issue is the lack of standardised communication protocols. Different cloud service providers may use different security protocols and communication frameworks, which may cause customers and service providers to encounter obstacles when sharing security incident data, such as delayed responses (Abdulsalam & Hedabou, 2021; Kumar et al., 2021). There is also insufficient sharing of threat intelligence. Many cloud service providers do not publicly share all relevant data when dealing with security threats. The reasons for doing so may include protecting trade secrets and avoiding potential reputation risks. However, this insufficient information sharing will prevent other customers and partners from quickly grasping the latest security trends and making it difficult to respond to similar security threats promptly.

Communication delays are also a challenge. When a security incident occurs, fast communication is essential. However, the communication response time of cloud service providers

 doi:10.20944/preprints202501.0716.v1

may be affected by factors such as service scale and technical support capabilities. This delay may cause the incident to spread and have a more serious impact.

3.2.2. Virtual Network Limitations

In cloud computing systems, communication occurs not only over physical networks but also heavily relies on virtualized networks. These virtual networks, logically built on top of physical infrastructure, enable efficient interaction between virtual machines (VMs) by establishing virtual connections. Through software-based network components—such as virtual bridges, routers, and software-defined network configurations—multiple VMs on the same host can communicate seamlessly, allowing for flexibility and data isolation. However, the adoption of virtualized networks also introduces distinct security challenges.

Firstly, because virtual network traffic is outside the protective scope of physical network defences, traditional security tools like firewalls and intrusion detection systems (IDS) often cannot monitor virtualized network traffic. This limitation makes malicious activities within virtual networks harder to detect and contain (Lim et al., 2019). Standard IDS and intrusion prevention systems rely on identifiable traffic and behaviour patterns to recognize anomalies and detect potential attacks. However, the isolated and dynamic nature of virtual networks impedes these tools from effectively capturing data flows between VMs, reducing their preventive effectiveness. This limitation heightens the risk of successful malicious attacks, posing a notable threat to data security in cloud environments.

Moreover, virtualized networks are commonly shared by multiple VMs, which increases susceptibility to various network-based attacks. For instance, attackers might exploit the shared nature of virtual networks to launch denial-of-service (DoS) attacks, disrupting regular services by consuming network resources. Additionally, virtual network spoofing (such as ARP spoofing) and traffic sniffing are significant concerns. Attackers can extract sensitive data by injecting false data or intercepting network traffic. In cases of malicious sniffing and spoofing, encryption keys and other sensitive information in transit are at high risk of theft, potentially resulting in costly data breaches, especially if the data includes personal or proprietary information.

In conclusion, while virtualized networks enhance the flexibility and scalability of cloud environments, they introduce specific security concerns. Therefore, cloud service providers and users must implement targeted security measures to identify and protect against potential attacks in virtualized networks during cloud environment design and deployment.

3.3. Future Potential of Cloud Computing Security

Cloud computing security has great potential in the future. With the continuous advancement of cloud technology and the increasing number of network threats, I believe that cloud security will continue to evolve and meet new challenges. As for the prediction of its future potential, I will divide it into four parts.

The first is security protection based on artificial intelligence and machine learning: As time goes by, network threat intelligence and hacker attack techniques become more and more complex, and traditional static security protection methods will become increasingly difficult to meet future security needs. AI and ML will become the core of cloud security. This threat detection system that automatically identifies abnormal behaviours, detects potential threats in real-time and responds to attacks promptly can help cloud organisations defend against a series of complex attacks such as APT more intelligently by constantly learning and adapting to new attack patterns (Shirgaonkar et al., 2022; Nayyar et al., 2021).

The second is the research and development of quantum computing security protection. With the rise of quantum computing technology, traditional encryption algorithms will gradually become vulnerable and unable to resist the cracking capabilities of quantum computing. To cope with this potential threat situation, cloud security may develop in the direction of quantum security, using quantum-resistant cryptographic algorithms and protocols to ensure data security in quantum

 doi:10.20944/preprints202501.0716.v1

computing environments. In the future, cloud service providers may provide quantum encryption options to enhance the long-term confidentiality of data (Parast et al., 2021; Shah et al., 2022).

Automated threat response and recovery is also a major potential direction. In the future, automated security responses will be more mature, and the response time for security incidents can be reduced by automatically detecting, isolating and processing threats (Sampson & Chowdhury, 2021). The cloud security platform will also realise a fully automated response system, including automatic repair, data recovery and real-time log auditing, making threat management and incident response more efficient and reducing the need for human intervention.

The fourth is the application of smart contracts in security protocols. In the future, perhaps smart contracts can realise automated security protocol execution in cloud computing. This smart contract-based security protocol can enhance the security of data transmission and transactions in the cloud environment, ensure that all parties follow predetermined security standards, and help achieve secure data exchange in a decentralised environment.

4. Discussion on Security Countermeasures

4.1. Security Countermeasure

Cloud computing has revolutionised the way data is preserved, shared, and retrieved (Infopark.in, 2024). However, in addition, it has brought a number of serious security concerns. Therefore, several countermeasures have been implemented against such threats seeking to compromise sensitive data, service integrity, and unauthorised access (Dawood et al., 2023). These are concerning malware injection, data breaches, account hijacking, denial of service, and insecure APIs.

Identity and Access Management (IAM) is undoubtedly an essential component of cloud security. It controls user access and ensures that cloud resources only interact with authorised users or systems. Multi-factor authentication (MFA) is a crucial element of IAM that involves multiple verification factors, and biometric authentication, such as device-based tokens, and passwords, for increased security (Dawood et al., 2023; Sharma et al., 2021). For example, Google Authenticator and hardware-based tokens such as YubiKeys add further levels of security, making it far more difficult for attackers to break in even when only one component is compromised. Single sign-on (SSO) simplifies user access by allowing authentication across numerous services with a single set of credentials, reducing password exhaustion and the risk of vulnerabilities (ElazarK, 2023). This also reduces insider threats and limits the possibility of privileges being misused either accidentally or intentionally.

Encryption is another critical measure to secure data, both in transit and at rest. Symmetric encryption algorithms, like AES-256, ensure high security with the different keys, making data unreadable for unauthorised users. As for data in transit, protocols like Transport Layer Security (TLS) encrypt communications, such as the ones over HTTPS, against interceptors and eavesdroppers (Khader and Karam, 2023; Singhal et al., 2020). At rest, server-side encryption solutions which are provided by cloud providers, for example, AWS Key Management Service (KMS), ensure that even in case physical servers are compromised, data will not be disclosed. Data masking is an enhancement on encryption where actual data is substituted with unreal yet functional look-alikes, especially within unproductive environments where testing or analytics occurs, reducing exposure but not affecting functionality.

Firewalls and Intrusion Detection Systems (IDS) are the essential elements of network traffic monitoring and control. Firewalls block unauthorised access to any network by filtering out incoming and outgoing traffic based on predetermined security rules. Intrusion detection systems, on their part, continuously monitor networks for suspicious activities. Both are quite efficient in identifying and preventing malware injection or distributed denial of service (DDoS) attacks that may cripple cloud systems (Ahanger and Aljumah, 2020).

 doi:10.20944/preprints202501.0716.v1

Regular mechanisms for data backup and recovery go a long way in assuring that business operations remain uninterrupted. The use of regular backups and multi-regional data replication is considered important in building resiliency within an organisation so that restoration can easily be done by the organisation in case of a disaster such as data loss due to either a cyber-attack or system failure (Alouffi et al., 2021).

Zero Trust Architecture (ZTA) introduces a new system in the field of cloud security by eliminating the trusting assumption within a network. Instead, every user, device, or application must be continuously verified and checked before being granted access. This approach uses principles such as micro-segmentation, dividing the network into smaller, isolated zones, and enforcing strict access controls for each. Device health checks apply to organisational security policies requiring updated antivirus software or encrypted storage. Using the least-privilege principle, ZTA confines a user or device to access the minimum possible number of resources. This greatly reduces the potential damage there could be in case of a breach. For instance, even if an attacker can gain access to one part of the network, he cannot move laterally inside to more critical parts thanks to micro-segmentation (Tan, 2023).

Blockchain technology is increasingly being used to enhance security in cloud computing. Its decentralised and fixed nature brings incomparable transparency and accountability. Each transaction or access event is recorded in a blockchain ledger, which cannot be changed or manipulated. Therefore, the integrity of the data is guaranteed, while auditing processes are easier. Furthermore, blockchain-based identity management systems avoid depending on centralised identity providers which reduces risks of credential thefts or tampering. Cryptographic hashing techniques associated with blockchain further extend the verification and integrity of the data stored in the cloud.

4.2. Proposed Countermeasure

Cloud Computing services bring a lot of conveniences and benefits to the users, but security issues are indeed a major criticism of the cloud computing service and this also affects the users' confidence in using the technology of cloud computing. Therefore, we need to take advanced and dynamic countermeasures to deal with complex and evolving security threats in cloud environments. For example, using artificial intelligence, blockchain and adaptive authentication mechanisms, which have become key countermeasures to reduce risks, and strengthen data protection against insider threats, credential leakage and unauthorised access.

One important aspect is that Artificial Intelligence (AI) plays a key role in the security strategy of cloud security services. It provides tools that are used to analyse large amounts of data at scale, learn from security events and respond to threats in real-time as well as identify the potential vulnerabilities and predict threats before they occur. This is because using AI-driven access control can detect anomalies that human analysts may miss, and this helps to build the cloud environment more robust and less vulnerable to attacks (Oduri, 2019). AI-driven access control provides dynamic security by evaluating user behaviour and background factors such as devices, locations, and login times. By evaluating these variables, AI can identify abnormal patterns and adjust access rights, thereby reducing the risks associated with internal threats and leaked credentials. It is well known that cybercriminals now use advanced technologies including machine learning and automation to attack. Therefore, we need to implement and deploy machine learning models that can continuously monitor and analyse cloud users' login time and capture their device type and geographic location to establish patterns of normal user behaviour. In this situation, the system under AI-driven control will adjust the access privileges or require additional verification when the system detects unusual activities such as a user accessing sensitive files from an unusual location from the user side to reduce potential security risk. Continuous monitoring and adjusting the access based on real-time behaviour may help to reduce the risk of insider threats and credential compromise significantly. However, AI-driven control cannot completely cover all security vulnerabilities, so if AI-driven access control

 doi:10.20944/preprints202501.0716.v1

is combined with traditional security measures, it can more comprehensively deal with diverse threats. (Olabanji et al., 2024).

Another significant point is about the Automated Failover System with Malicious IP record which can improve the elasticity of the cloud services provided by ensuring the cloud service provider remains operational even if an attack happens or facing system failure. The system can block repeated attempts from flagged sources by maintaining the record of malicious IP addresses. These functions ensure that the key service can remain available and secure which may result in minimising the downtime of cloud service and also reduce the risk of distribution of target attack. The implementation of an Automated Failover system is about configuring a server load balancer to the system which functions in detecting the overloads of failures automatically, then it will take action in switching the traffic flow to backup servers in an instant way (Amazon Web Services, 2019). At the same time, through an integrated threat intelligence system, the maintenance and upgrading of the record of malicious IP supports the function of detecting malicious activity. The system will log the offending IP block the IP from re-assessing the service and generate an alert notification to the administrator to ensure a quick response to any unusual pattern (Usman et al., 2021). The implementation of an Automated Failover System with a Malicious IP Record may ensure the cloud service remains accessible for the cloud service users even if the cloud provider side is facing unexpected failures or attacks and prevents repeat access from malicious IPs. The prevention of repeat access from malicious IPs helps to reduce and minimise recurring threats and downtime. The system will ultimately improve service reliability and safety while reducing operational costs associated with extended service interruptions.

Additionally, countermeasures can be used in cloud security also including the Blockchain-based Cloud Security which uses the blockchain decentralised architecture. Decentralised architecture provides secure identity management and ensures data integrity. Decentralised architecture provides secure identity management and ensures data integrity. Blockchain technology strengthens identity verification, reduces the risk of unauthorised access and ensures all modifications to data are fully traceable by a decentralised approach since this technology enables a transparent and tamper-proof record of the action made by users by recording every transaction on an immutable ledger (Velmurugadass et al., 2020). By implementing the Blockchain architecture into cloud security, we can deploy the blockchain-based system within the cloud service environment as a consortium blockchain and grant access to specific stakeholders. It can create an immutable trail of transactions by recording sensitive identity credentials and data on the blockchain. The system can automate access control policies such as only permitting authorised action and receding any data by using smart contracts and the administrator of the cloud system can easily audit these blockchain records to verify the source and legitimacy of all actions. Blockchain-based cloud security makes identity management more secure and decentralised and helps to reduce vulnerabilities associated with centralised systems. Any unauthorised modification is allowed to be immediately traceable since the immutable transaction records enhance data integrity. This transparency provides stronger auditability ensures compliance with the regulatory standard and builds user trust in the security of the cloud environment provided.

Furthermore, applying the Zero Trust Architecture (ZTA) model integrated with AI-driven behavioural analytics into cloud security is also one of the countermeasures used to keep the cloud environment secure and responsive. Insider threats, credential misuse, and unauthorised access are particularly effective when using an advanced Zero Trust Architecture (ZTA) model integrated with AI-driven behavioural analytics (Ahmadi, 2024). This model makes security more adaptive and responsive by dynamically adjusting access permissions based on user behaviour patterns and real-time risk assessments, while continuously verifying identities and identifying anomalies that may indicate potential security threats (Grobler, Gaire and Nepal, 2021). Login frequency, device usage and access location were gathered by the Advance ZTA with AI and Behavioural data to establish a user-specific baseline. The machine learning models analyse data in real-time which the models will learn from normal patterns to detect anomalies (Butt et al., 2020). The system will access permission,

 doi:10.20944/preprints202501.0716.v1

prompt for additional authentication or restrict access temporarily when unusual activity is detected. Continuous monitoring and model re-evaluation improve the accuracy of threat detection and response over time. Early detection of insider threats and credential misuse provided by the advanced ZTA approach enhances security through AI-driven behavioural analytics. To create a balanced and user-friendly security environment, the system needs to proactively respond to suspicious behaviour, reducing unauthorised access risk and containing threats quickly to benefit users by providing them with a seamless experience for routine action while security intensifies high-risk activities.

In the same vein, Adaptive Multi-Factor Authentication (MFA), as an integral component of the Zero Trust Architecture (ZTA) model integrated with AI-driven behaviour analytics, adjusts authentication requirements based on the risk level of each access attempt to provide a dynamic, context-sensitive approach to the cloud security. Adaptive MFA strikes a balance between usability and strong security because this countermeasure effectively reduces user friction, while it also improves security in high-risk scenarios by reducing the steps of routine operations and performing stricter verification for sensitive access (Mostafa et al., 2023). To implement adaptive MFA in cloud security, cloud service systems need to adjust the authentication steps based on the risk level of each operation. For example, the low-risk activities only need users to key in the password or one-time code for verification, while when facing a higher-risk action such as users trying to access sensitive data, the system will require the users to go through biometric verification in addition to a password. The combination of machine learning and the system are more effective in tracking the login pattern and aloud adjustment of the security level dynamically to ensure only authorised individuals access critical resources. The implementation of Adaptive MFA prevents unauthorised access to sensitive information and enhances security for high-risk operations through layered authentication. Cloud service users can enjoy a simplified experience for daily tasks with minimal friction while they still benefit under a strong and reliable cloud security framework since this countermeasure reduces the risk of credential compromise and enhances overall the cloud security group without sacrificing usability (Mostafa et al., 2023).

In conclusion, innovative and dynamic solutions are needed to safeguard user trust and data integrity on the cloud, even though cloud computing offers substantial benefits and convenience for users, cloud security is important in cloud service. Therefore, the key strategies to ensure the security environment such as AI-driven access control, Automated Failover Systems, Blockchain-based security, Zero Trust Architecture and Adaptive Multi-Factor Authentication play a vital role in protecting against evolving cyber threats, inside risks and unauthorised access. Cloud service providers can create resilient defence frameworks that address diverse vulnerabilities. Cloud security is critical to prevent data breaches and also increase user confidence in the cloud service provided, thereby ensuring the continued growth and safe adoption of cloud technology.

5. Conclusion

Overall, although cloud computing brings many conveniences to users, security issues remain crucial for maintaining user trust and data protection. Therefore, it's essential to use advanced security measures to keep cloud environments safe. AI-driven access control can monitor user behaviour dynamically, reducing the risks of internal threats and credential leaks. The automated failover system records malicious IP addresses, ensuring services remain available even if there's an attack or system failure. Blockchain technology protects identity management and data integrity through decentralisation, providing transparent and unchangeable records that help with compliance and build user trust. The Zero Trust Architecture requires users and devices to go through multiple levels of verification, limiting unauthorised access. Even if an intrusion happens, it prevents attackers from moving freely across the network, reducing the damage. Adaptive Multi-Factor Authentication (MFA) adjusts verification steps based on risk level, balancing security and user experience. Low-risk actions have simpler verification, while sensitive data access has stricter checks. Together, these measures form a layered defence system, helping cloud providers protect

 doi:10.20944/preprints202501.0716.v1

data in a complex threat environment and enhancing user confidence. With these innovative security methods, the cloud environment can not only defend against external attacks but also improve its resilience and adaptability, creating a strong foundation for the long-term, safe use of cloud technology.

We understand that while cloud computing brings convenience, it also faces security risks such as data breaches and malware attacks. This reminds us of the importance of data protection and access control. We have learned about some key security measures, such as Identity and Access Management (IAM), encryption, firewalls, and Intrusion Detection Systems (IDS), which help secure the cloud environment. Additionally, advanced methods like Zero Trust Architecture can effectively limit unauthorized access, enhancing data security and user trust. This knowledge helps us better understand the importance of cloud security and guides us to strengthen data protection in practical applications.

Some key security measures were mentioned, helping us understand how to protect the security of cloud environments. First, Identity and Access Management (IAM) is a basic technology for cloud security. By controlling user identities and access permissions, it can effectively prevent unauthorized users from accessing sensitive data. IAM systems can use methods like Multi-Factor Authentication (MFA) to ensure that only verified users can access critical resources. In addition, firewalls and Intrusion Detection Systems (IDS) can help filter network traffic and monitor suspicious activities, further reducing the risk of malicious attacks. The combined use of these security technologies can enhance the overall defence capabilities of the cloud computing environment.

Explained the importance of data encryption. Encryption can ensure data is kept private during the transmission and storage process, even if a leak happens, unauthorized persons cannot read data content. Combined with data backup and disaster recovery measures, it can quickly recover when data is lost or under attack, ensuring business continuity and reliability. Moreover, technical measures like data segmentation and network isolation are important means to prevent attack spreading.

Besides these traditional measures, also introduced more advanced Zero Trust Architecture. This method emphasizes that it needs multi-level verification before accessing any resource, and divides strict access permissions in the network, ensuring even if intrusion occurs, attackers are difficult to move freely and expand attack range. Zero Trust Architecture through continuous verification and strict control access, greatly improves data security and enhances users' trust in cloud environments.

Furthermore, mentioned using blockchain technology to protect data integrity, through unchangeable records to guarantee operation transparency and credibility. This decentralized technology can further enhance users' confidence in data security. All operations recorded by blockchain can be traced back, which is especially suitable for data storage and management needing high compliance and transparency.

Through learning, we realize that in complex threat environments, multi-layer defence strategies and advanced protection technologies of cloud computing security are extremely important. We should adopt these security measures in practical applications to protect data, including IAM, encryption, firewall, Zero Trust Architecture, etc., further strengthening the protection of data, and ensuring the security and reliability of cloud services. This knowledge helps us fully understand the necessity of cloud computing security and also makes us more clearly aware of how to take more effective measures in practice to deal with constantly changing security challenges.

References

Abdulsalam, Y.S. and Hedabou, M. (2021). Security and Privacy in Cloud Computing: Technical Review. Future Internet, [online] 14(1), p.11. doi:https://doi.org/10.3390/fi14010011.

Ahanger, T. and Aljumah, A. (2020). Cyber Security Threats, Challenges and Defense Mechanisms in Cloud Computing. *IET Communications*, [online] 14(7). doi:https://doi.org/10.1049/iet-com.2019.0040.

Ahmad, W., Rasool, A., Javed, A.R., Baker, T. and Jalil, Z. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, [online] 11(1), p.16. doi:https://doi.org/10.3390/electronics11010016.

Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, 15, 148-167. https://doi.org/10.4236/jis.2024.152010.

Ahmadi, S. (2024). *Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities*. [online] Ssrn.com. Available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4725283_code6402189.pdf?abstractid=4725283&mirid=1&type=2 [Accessed 12 Nov. 2024].

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

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

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. IEEE Access, [online] 9(1), pp.1–1. doi:https://doi.org/10.1109/access.2021.3073203.

Amazon GuardDuty User Guide Amazon GuardDuty. (n.d.). Available at: https://docs.aws.amazon.com/pdfs/guardduty/latest/ug/guardduty-ug.pdf.

Amazon Web Services. (2019). *Automated Disaster Recovery using CloudEndure | Amazon Web Services*. [online] Available at: https://aws.amazon.com/cn/blogs/architecture/automated-disaster-recovery-using-cloudendure/ [Accessed 12 Nov. 2024].

Amazon.com. (2024). *Security best practices for Amazon S3 - Amazon Simple Storage Service*. [online] Available at: https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html#.

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

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

Basan, M. (2024). *Top Cloud Security Issues: Threats, Risks, Challenges & Solutions*. [online] eSecurity Planet. Available at: https://www.esecurityplanet.com/cloud/cloud-security-threats/.

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

Butt, U.A., Mehmood, M., Shah, S.B.H., Amin, R., Shaukat, M.W., Raza, S.M., Suh, D.Y. and Piran, M.J. (2020). A Review of Machine Learning Algorithms for Cloud Computing Security. Electronics, [online] 9(9), p.1379. doi:https://doi.org/10.3390/electronics9091379.

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

Cloudflare (2024). *What is a next-generation firewall (NGFW)?* [online] Cloudflare.com. Available at: https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/.

Cloudsecurityalliance.org. (2024). *Security as a Service Working Group | CSA*. [online] Available at: https://cloudsecurityalliance.org/research/working-groups/security-as-a-service [Accessed 3 Nov. 2024].

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M. and Rehman, S.U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*, [online] 15(11), pp.1–33. doi:https://doi.org/10.3390/sym15111981.

Díaz de León Guillén, M.Á., Morales-Rocha, V. and Fernández Martínez, L.F. (2020) 'A systematic review of security threats and countermeasures in SaaS', *Journal of Computer Security*, 28(6), pp. 635–653. doi:10.3233/JCS-200002.

Dissanayake, N., Jayatilaka, A., Zahedi, M. and Babar, M.A. (2021). Software security patch management—A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, [online] 144, p.106771. doi:https://doi.org/10.1016/j.infsof.2021.106771.

docs.aws.amazon.com. (n.d.). What are AWS WAF, AWS Shield, and AWS Firewall Manager? - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced. [online] Available at: https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html#waf-intro.

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

ElazarK (2023). *What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction.

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

Gaur, L., Arora, G. K., & Jhanjhi, N. Z. (2022). Deep learning techniques for creation of deepfakes. In *DeepFakes* (pp. 23-34). CRC Press.

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

Grobler, M., Gaire, R. and Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. Frontiers in Big Data, 4. doi:https://doi.org/10.3389/fdata.2021.583723.

Hong, J.B., Nhlabatsi, A., Kim, D.S., Hussein, A., Fetais, N. and Khan, K.M. (2019). Systematic identification of threats in the cloud: A survey. *Computer Networks*, [online] 150, pp.46–69. doi:https://doi.org/10.1016/j.comnet.2018.12.009.

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., Niazi, M., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2023). Toward a readiness model for secure software coding. *Software: Practice and Experience*, *53*(4), 1013-1035.

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

 doi:10.20944/preprints202501.0716.v1

IBM (2023). *What is an intrusion prevention system (IPS)? | IBM*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/intrusion-prevention-system.

IBM (2024). *Cost of a Data Breach 2024*. [online] IBM. Available at: https://www.ibm.com/reports/data-breach.

IEEE Digital Privacy (2023). Ethical Issues Related to Data Privacy and Security: Why We Must Balance Ethical and Legal Requirements in the Connected World - IEEE Digital Privacy. [online] digitalprivacy.ieee.org. Available at: https://digitalprivacy.ieee.org/publications/topics/ethical-issues-related-to-data-privacy-and-security-why-we-must-balance-ethical-and-legal-requirements-in-the-connected-world.

IMI (2024). *Identity and Access Management Tools - Identity Management Institute®*. [online] Identity Management Institute®. Available at: https://identitymanagementinstitute.org/identity-and-access-management-tools/ [Accessed 2 Nov. 2024].

Infopark. in. (2024). *Classic Examples of Cloud Computing that are keeping the world at our Fingertips – InfoparkBlog*. [online] Available at: https://blog.infopark.in/index.php/2021/09/26/classic-examples-of-cloud-computing-that-are-keeping-the-world-at-our-fingertips/ [Accessed 10 Nov. 2024].

Javed, D., Jhanjhi, N. Z., & Khan, N. A. (2023, April). Football analytics for goal prediction to assess player performance. In *Innovation and Technology in Sports: Proceedings of the International Conference on Innovation and Technology in Sports,(ICITS) 2022, Malaysia* (pp. 245-257). Singapore: Springer Nature Singapore.

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

Josic, D., Basic, M. and Zgrablic, L. (2024). 35TH DAAAM INTERNATIONAL SYMPOSIUM ON INTELLIGENT MANUFACTURING AND AUTOMATION SECURITY PRINCIPLES IN CLOUD COMPUTING. [online] doi:https://doi.org/10.2507/35th.daaam.proceedings.xxx.

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

Justinha (2024). *Deployment considerations for Microsoft Entra multifactor authentication - Microsoft Entra ID*. [online] Microsoft.com. Available at: https://learn.microsoft.com/en-my/entra/identity/authentication/howto-mfa-getstarted.

Keary, T. (2023). *Report shows 92% of orgs experienced an API security incident last year*. [online] VentureBeat. Available at: https://venturebeat.com/security/report-shows-92-of-orgs-experienced-an-api-security-incident-last-year/ [Accessed 24 Nov. 2024].

Khader, M. and Karam, M. (2023). Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis. [online] 8(6), pp.105–105. doi:https://doi.org/10.3390/data8060105.

Konatham, B., Simra, T., Amsaad, F., Ibrahem, M. I., & Jhanjhi, N. Z. (2024). A Secure Hybrid Deep Learning Technique for Anomaly Detection in IIoT Edge Computing. *Authorea Preprints*.

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

Kumar, R. and Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, [online] 33, pp.1–48. doi:https://doi.org/10.1016/j.cosrev.2019.05.002.

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

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

Microsoft (n.d.). [online] What is Microsoft Defender for Cloud? Available at: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction.

Moitrayee Chatterjee, Prerit Datta, Faranak Abri, Akbar Siami Namin and Keith S. Jones (2020). [online] Cloud as an Attack Platform. Available at: https://arxiv.org/pdf/2006.07914.

Mostafa, A.M., Ezz, M., Elbashir, M.K., Alruily, M., Hamouda, E., Alsarhani, M. and Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Applied sciences*, 13(19), pp.10871–10871. doi:https://doi.org/10.3390/app131910871.

msmbaldwin (2024). *Azure identity & access security best practices*. [online] Microsoft.com. Available at: https://learn.microsoft.com/en-my/azure/security/fundamentals/identity-management-best-practices

Mythili, K. and Rajalakshmi, S. (2022) 'Enhancing Role Based Access Control with Privacy in Cloud Computing', Turkish Online Journal of Qualitative Inquiry, 13(1), pp. 204–211. Available at: https://research-ebsco-com.ezproxy.taylors.edu.my/linkprocessor/plink?id=aa4502ff-ede5-369f-958b-1c857c5a8e74 (Accessed: 2 November 2024).

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

Oduri, S. (2019). Integrating Ai Into Cloud Security: Future Trends And Technologies. [online] 16(1), p.386. Available at: https://www.webology.org/data-cms/articles/20240905063955pmWEBOLOGY%2016%20(1)%20-%2035.pdf.

Olabanji, S.O., Marquis, Y., Adigwe, C.S., Ajayi, S.A., Oladoyinbo, T.O. and Olaniyi, O.O. (2024). *AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection*. [online] Social Science Research Network. doi:https://doi.org/10.2139/ssrn.4709384.

PaloAlto Networks (2024). *IPS. vs. IDS vs. Firewall: What Are the Differences?* [online] Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips [Accessed 9 Nov. 2024].

Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B. and Hakak, S. (2021). Cloud Computing Security: A Survey of Service-based Models. *Computers & Security*, [online] 114, p.102580. doi:https://doi.org/10.1016/j.cose.2021.102580.

Purna, C., Reddy, L., Apoorva, D., Jaleel Basha, S., Manikanta, G., Chandarao, N. and Ambarisha, M. (n.d.). Private Document Vault with server side Encryption Using Cloud AWS. [online] Available at: http://ijirse.com/wp-content/upload/2023/09/776.pdf

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

RiskRecon (2023). Shared Responsibility Model in Cloud Computing: What You Need to Know. [online] Riskrecon.com. Available at: https://blog.riskrecon.com/shared-responsibility-model [Accessed 4 Nov. 2024].

Rosenberg, M. et al. (2024) 'Edo4siem - a Procedure Model for the Implementation of Security Information and Event Management Systems in Organisations', IADIS International Journal on Computer Science & Information Systems, pp. 31–47. Available at: https://research-ebsco-com.ezproxy.taylors.edu.my/linkprocessor/plink?id=fcdba84e-775f-3dcd-8d2f-f2af852d11a0 (Accessed: 4 November 2024).

Routavaara, I. (2020). Security monitoring in AWS public cloud. [online] Available at: https://www.theseus.fi/bitstream/handle/10024/341640/Opinnaytetyo_Routavaara_Ilkka.pdf?sequence=2.

Sampson, D., & Chowdhury, M. M. (2021). The Growing Security Concerns of Cloud Computing. *Proceedings of the 2021 IEEE International Conference on Electro Information Technology (EIT)*, Mt. Pleasant, MI, USA, 14–15 May 2021. https://ieeexplore.ieee.org/abstract/document/9491902

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). *17 Security Risks of Cloud Computing in 2024*. [online] Available at: 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

Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). Enabling Explainable AI in Cybersecurity Solutions. In *Advances in Explainable AI Applications for Smart Cities* (pp. 255-275). IGI Global.

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

Shirgaonkar, M., Shinde, A., Sankpal, P., and Gutte, V. (2022) Cloud Computing Security using Cryptographic Algorithms. Published in: 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), IEEE. Available at: https://ieeexplore.ieee.org/document/9753902.

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

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

Srilatha, D. and Thillaiarasu, N. (2023) 'Implementation of Intrusion detection and prevention with Deep Learning in Cloud Computing', Journal of Information Technology Management, 15, pp. 1–18. doi:10.22059/jitm.2022.89407.

Sun, P.J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges and Solutions. IEEE Access, 7, pp.1–1. doi:https://doi.org/10.1109/access.2019.2946185.

Talluri, S. and Teja Makani, S. (2023). Managing Identity and Access Management (IAM) in Amazon Web Services (AWS) . [online] Available at: https://www.researchgate.net/profile/Sai-Teja-Makani/publication/378794145_Managing_Identity_and_Access_Management_IAM_in_Amazon_Web_Services_AWS_USA/links/65e9c29cbe5f372f64c4edb6/Managing-Identity-and-Access-Management-IAM-in-Amazon-Web-Services-AWS-USA.pdf.

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.

Tan, K.H. (2023). Mitigating Insider Threats in AWS: A Zero Trust Perspective. figshare. [online] doi:https://doi.org/10.1184/R1/23931384.v1.

Usman, N., Usman, S., Khan, F., Jan, M.A., Sajid, A., Alazab, M. and Watters, P. (2021). Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics. *Future Generation Computer Systems*, 118, pp.124–141. doi:https://doi.org/10.1016/j.future.2021.01.004.

Velmurugadass, P., Dhanasekaran, S., Shasi Anand, S. and Vasudevan, V. (2020). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*. doi:https://doi.org/10.1016/j.matpr.2020.08.519.

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

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

www.okta.com. (2024). *What Is Role-Based Access Control (RBAC)? | Okta*. [online] Available at: https://www.okta.com/identity-101/what-is-role-based-access-control-rbac/.

Yanamala, A.K.Y., 2024. Emerging Challenges in Cloud Computing Security: A Comprehensive Review. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4), pp.448-479.

Zaman, N., Ghazanfar, M. A., Anwar, M., Lee, S. W., Qazi, N., Karimi, A., & Javed, A. (2023). Stock market prediction based on machine learning and social sentiment analysis. *Authorea Preprints*.