Article

Not peer-reviewed version

Cloud Security: Counteracting Evolving Threats in a Digital Age

Chan Jian Jern , Chan Wei Yan , Ho Hoong Khuan , Huang Enze , Jason Tang Kwong Wee , Lee Zu Han , Leong Yu Xuan , Lim Lai Soon , Ong Wei Shih , Phoon Chun On , Wong Jun , Siva Raja Sindiramutty *

Posted Date: 7 January 2025

doi: 10.20944/preprints202501.0514.v1

Keywords: Cloud Computing Security; Zero-Trust Architecture; AI-Augmented Threat Detection; Data Leakage Prevention; Multi-Cloud Strategies

Article

Cloud Security: Counteracting Evolving Threats in a Digital Age

Chan Jian Jern, Chan Wei Yan, Ho Hoong Khuan, Huang Enze, Jason Tang Kwong Wee, Lee Zu Han, Leong Yu Xuan, Lim Lai Soon, Ong Wei Shih, Phoon Chun On, Wong Jun and Siva Raja Sindiramutty *

Taylor's University, Malaysia

* correspondence: magan.shiva91@gmail.com

Abstract: This report is to investigate the development of cloud computing and its security paradigms, highlighting key components such as data, applications, operating systems, virtualization, servers, storage, and networking, which form the foundation of cloud security. It explores the threats inherent in cloud environments, including account hijacking, malware, data leakage, DoS/DDoS attacks, and social engineering, detailing their impact and countermeasures. Notable security technologies like encryption, Identity and Access Management (IAM), cloud firewalls, and disaster recovery planning are discussed as critical safeguards. Limitations of cloud computing security, including bandwidth issues, redundancy challenges, and control constraints, are analysed alongside emerging trends like AI-driven threat detection, the adoption of zero-trust security models, and unified multi-cloud security approaches. The report proposes advanced countermeasures, including enhanced zero-trust models with behavioural biometrics and adaptive honeypots, as well as AI-augmented threat detection systems utilizing neural networks and reinforcement learning. The findings underscore the importance of continuous innovation and adaptive strategies in cloud computing security to mitigate evolving threats and ensure secure, resilient cloud infrastructures. Future advancements in regulatory compliance, AI integration, and predictive analytics will further shape the trajectory of cloud security in the face of growing technological complexities.

Keywords: Cloud Computing Security; Zero-Trust Architecture; AI-Augmented Threat Detection; Data Leakage Prevention; Multi-Cloud Strategies

1.0. CLOUD COMPUTING BACKGROUND

1.1. Cloud Computing Development History

In a 1965 publication, Christopher Strachey explicitly introduced the idea of "virtualization." This was the beginning of cloud computing. Virtualization is the cornerstone and fundamental element of cloud computing development (Jayachander Surbiryala, 2019).

In the 1990s, computing expanded quickly, and companies like Cisco thrived. By making network services quick and simple to use, the expansion of the Internet has now benefited more users. Users will have access to more potent computing processing services because of certain significant companies beginning to create large-scale computing power technology at the same time (Jayachander Surbiryala, 2019).

In 2006, this was a pivotal point in the development of cloud computing. On August 9, 2006, Google CEO Eric Schmidt first introduced the concept of "Cloud Computing" at the Search Engine Conference (SESSanJose2006). That year saw the launch of Amazon's IaaS service platform, AWS (Jayachander Surbiryala, 2019).

 doi:10.20944/preprints202501.0514.v1

Although the concept of "cloud computing" was first proposed by AWS in 2006, the word was not formally adopted by the industry until 2008. The domestic cloud computing standard, Ali Cloud, began to prepare in that year (Ananna et al., 2023; Babbar et al., 2021). But the short two-year time difference also gives Amazon, the first to venture into this wild region, a natural advantage. At the height of the financial crisis, in early 2009, the US-based Salesforce company published its 2008 fiscal year annual report (Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023). The report showed that the company's revenue from cloud services topped $1 billion. Since then, cloud computing has become one of the most important areas for the growth and research of Internet companies and one of the most worrisome subjects in the computer industry (Jayachander Surbiryala, 2019).

With the emergence of a second tier that includes IBM, VMware, Microsoft, and AT&T, top-tier providers have steadily entered the cloud industry over the next few years. In 2011, Google announced the launch of GCP, marking the beginning of the same phase in the public cloud industry (Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023; Brohi et al., 2020). Although its CEO, Steve Ballmer, is still sluggish, Microsoft joined around 2010 (Jayachander Surbiryala, 2019).

As cloud computing technology gradually matures, manufacturers are offering security services via cloud service platforms. Security as a service is the collective term for a variety of additional security products and solutions that are offered directly through cloud services (Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023; Chesti et al., 2020). The Security Guidelines for Key Areas of Cloud Computing published by the Cloud Security Alliance (CSA) state (Khalil, 2014)

1.2. Cloud Computing Security Development

Cloud security has drawn increasing attention as cloud computing becomes more widely used, and both established and up-and-coming cloud computing and security businesses have introduced numerous cloud security technologies. However, the industry has yet to reach a clear consensus on "cloud security" from the concept, technology, and product, in contrast to the well-defined "cloud computing" (NISTSP 800-145 and ISO/EC Park 17788) (Khalil, 2014).

From the context of development analysis, "cloud security" related technologies can be divided into two categories:

Class provides protection for the use of cloud Computing services, namely security for using the cloud, also known as Cloud Computing Security, which is generally a new product category (Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023; Dogra et al., 2021). The class is derived from traditional security hosting services, that is, security provided from the cloud Service (also known as security-as-a-service (SECaaS)), There is usually a traditional security (Sama et al, 2022, Saleh et al, 2020) software or equipment production cloud.

 doi:10.20944/preprints202501.0514.v1

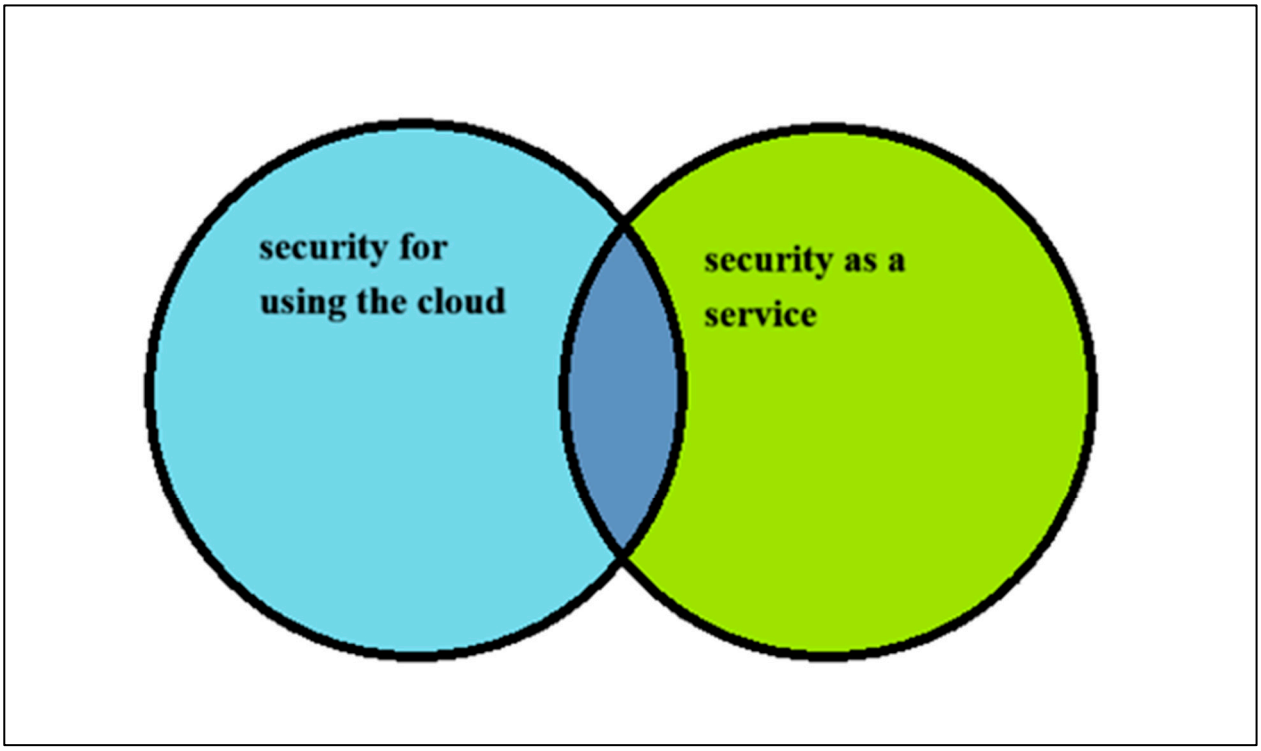

Figure 1. Cloud Computing Security Classification.

The overlap between the two cloud technologies is that the cloud service mode protects the use of cloud computing services.

1.3. Three components of the NIST Cloud Computing Security Reference Architecture

Service based on cloud model, deploy, and participating in three dimensions, such as the American national standards institute of technology (NIST) cloud computing security working group released in May 2013 the cloud computing security reference architecture (draft) gives the cloud computing reference architecture (NCC - SRA, NIST Cloud Computing Security Reference Architecture) (Fang Liu, 2011). Figure 1 shows cloud computing security classification.

Three dimensions make up the NIST Cloud Computing Security Reference Architecture.:

The three cloud computing service models: IaaS, PaaS, and SaaS. Cloud computing can be deployed using four different models: community, hybrid, private, and public. In cloud computing, there are five roles: auditor, agent, carrier, consumer, and provider. Figure 2 shows NIST Cloud Computing Security .

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2025 doi:10.20944/preprints202501.0514.v1

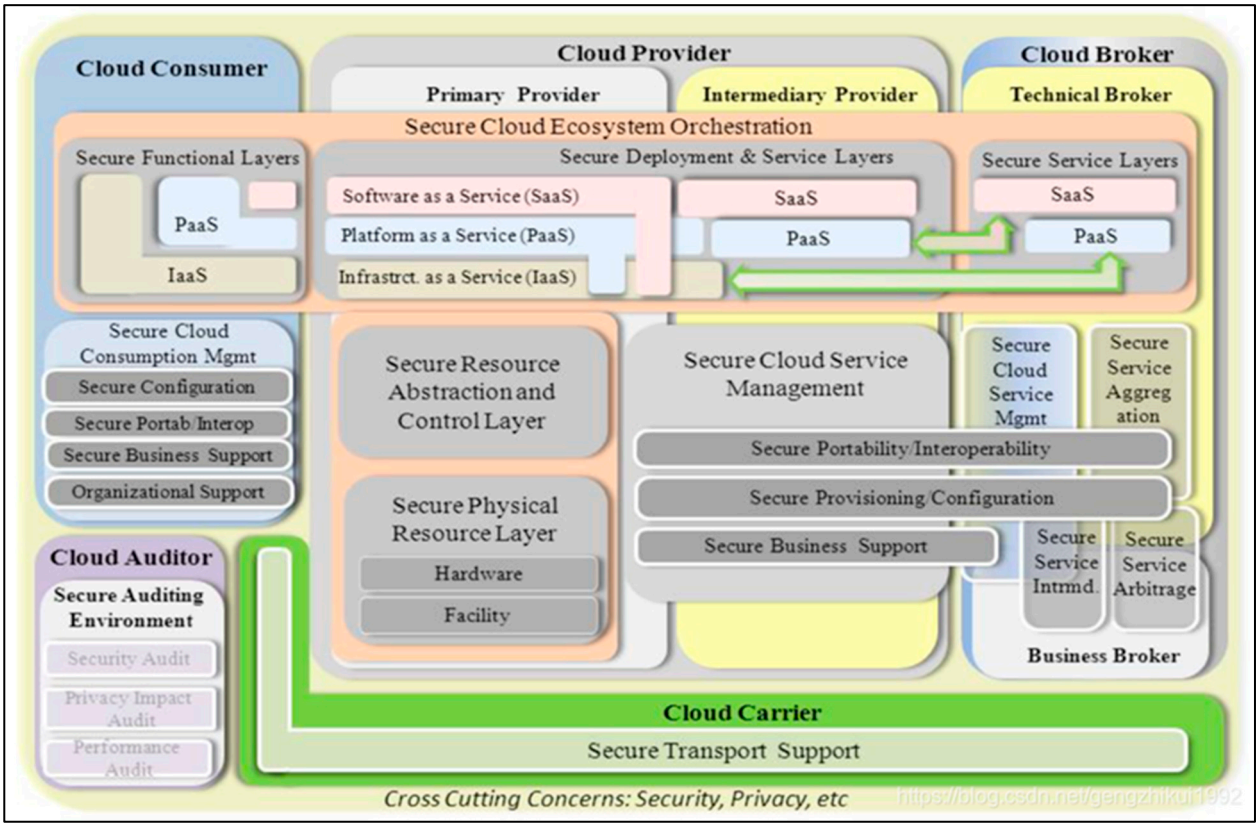

Figure 2. NIST Cloud Computing Security (Foster, 2013).

2.0. DETAILED DISCUSSION

2.1. Component

As defined by Deyan Chen and Hong Zhao (Deyan Chen, 2012), Cloud Computing Security, or often abbreviated as cloud security is a subset of security of computer and network that is managed by privacy-enhancing technology and regulated by a set of policy rules to safeguard the use of data, software applications, and related services that are outsourced to the cloud. As such, when we discuss about the components of cloud computing security, we are talking about a subset of components of cloud computing (Hussain et al., 2024; Fatima-Tuz-Zahra et al., 2020). IBM defined the components of cloud computing as data centres, networking capabilities, and virtualization (International Business Machines Corporation, 2024). However, this is too broad for what cloud computing security covers. Therefore, we can look at key components of cloud security, which separates cloud security into 7 components, namely data, applications, operating system, virtualization, servers, storage, and networking. We will discuss further what each of these components mean in the section below.

2.1.1. Data

Data are often referred to as larger amounts of unorganized information produced by a variety of sources such as sensors, mobile devices, social media, and IoT devices (Fabrizio Marozzo, 2022). In this case, these data would be on the cloud environment. Data can be separated into sensitive data and insensitive data (Jun et al., 2024; Gopi et al., 2021). Sensitive data are the upmost important component to be protected in cloud environment and should be always kept secure with limited access. Insensitive data on the other hand can be accessed by anyone but the integrity of the data should never be compromised.

2.1.2. Applications

 doi:10.20944/preprints202501.0514.v1

Applications, or sometimes called cloud applications are defined as software that runs natively on the cloud that are accessible to users via the Internet (Nazir, 2020). As these cloud applications often contains sensitive user data, it is crucial that the application itself is secure and does not contain any vulnerability that will lead to leak of data.

2.1.3. Operating System (OS)

Operating System is a system software that controls the hardware and software resources of a computer. The security of an OS is also very important as cloud computing supports various OS, therefore, if the computer itself is not secure, a secure cloud computing environment will not be achievable as well (Manchuri et al., 2024; Gouda et al., 2022). As cloud computing grows bigger, a concept of Web Operating System (WOS) has also emerged. A WOS is an interface that gives users access to various programs and applications that are entirely or partially hosted on the Internet (Zain Tahir, 2015). Although it may sound like conventional OS, a WOS doesn't interact with the system's hardware directly (Khan et al, 2020). This makes the security of an OS or WOS more important as they can be the weak link in cloud computing security, particularly when overlooked.

2.1.4. Virtualization

Virtualization means making a virtual replica of something, instead of the actual one. In the context of cloud computing, virtualization is the process of digitally reproducing an actual version of something (Ravichandran et al., 2024; Humayun et al., 2022). It enables numerous clients and organizations to share a single physical resource or application. Such technology enables a single hardware computing unit (host machine) to be divided into several virtual machines (Shukur, 2020). Even though these virtual machines act as a logically separated machine, crossover may still happen, which will lead to vulnerabilities in the host machine.

2.1.5. Servers

Servers or a cloud server, as defined by IBM (International Business Machines Corporation, 2024), is a robust physical or virtual infrastructure that is hosted remotely by a cloud service provider to achieve the functionality of delivering applications, processing data, or storing data. Ensuring the security of such physical or virtual infrastructure is crucial to maintaining a secure cloud environment due to the servers having direct access to the important data that is being processed or stored.

2.1.6. Storage

Storage, or more precisely cloud storage is when data is transmitted and stored on a remote storage device (Allan Liu, 2018). These stored data is maintained and backed up frequently to make them accessible to users over a network. Storage stores data used for cloud computing, therefore,

2.1.7. Networking

Networking on cloud computing, or better known as cloud networking, is a type of cloud infrastructure where an organization's networking resources are hosted in a private, public or hybrid cloud (Chellammal Surianarayanan, 2023). Cloud networking is essentially what enables cloud computing to be accessible everywhere. Therefore, the integrity and confidentiality of data during transmission must be protected.

2.2. Process

Investigating cloud computing security means understanding how cloud systems work, what risks they face, and how to protect them. Here's a straightforward explanation of the process:

1. Understand What Cloud Security Is

 doi:10.20944/preprints202501.0514.v1

Cloud security is about protecting data and applications stored on the internet (the "cloud") from being stolen or damaged. Think of it like locking your house but for your online data and apps. It includes rules, tools, and technology to keep everything safe.

2. Look at the Important Parts of Cloud Security

The information you store in the cloud like photos, documents, or business data. Sensitive data like passwords must be locked tight as well. The programs you use in the cloud and the software running on your computer or server need to be built securely to prevent hacking.

Virtualization: This means creating "virtual" computers inside one real computer to save space and resources. It's handy but can be risky if not done right.

Servers: The big computers where your cloud data lives. These need strong defences, just like a bank vault.

Storage: The "cloud hard drive" where data is saved. It must be backed up and secure to avoid losing information.

Networking: The connections that let you access the cloud. These should keep your data private and safe while traveling online.

3. Understand the Risks

There are risks like someone stealing your keys to break into your online accounts or even malware infections like viruses that can infect the cloud and steal or affect your data. There are also risks of data leaks where sensitive information is accidentally made public or stolen. It is also possible that DDoS attacks happens where someone floods the service with too much traffic which leads the entire system to overload and crash.

4. Learn About the Tools to Protect the Cloud

Tools to protect the cloud include encryption which scrambles data so only authorized people can read it. Firewalls and recovery plans can be put up so that barriers can block unauthorized access to cloud systems while backing up plans to recover data if they are lost. Another tool that can be used is Identity and Access Management, a system that only allows the right people to access that specific part of the cloud.

5. Recognize the Challenges

Some of the challenges include slow internet connection where a weak connection can affect cloud performance and security as well as if backup problems occur when data is not stored in proper places, it could be lost forever. Lack of control is also a common issue as businesses usually rely on third-party providers to manage their data, resulting a lesser control over what data they lost or affected.

Lack of Control: Businesses often rely on third parties (like cloud providers) to manage their data, which means less direct control.

2.3. Threat

Every organization and individual must deal with security concerns, threats, and obstacles. Although these terminologies are more complex, many people believe they all mean the same thing. You may better safeguard your cloud assets by being aware of their small variances. What are the security threats associated with cloud computing? The threat is the attacker who attempts to use that API to obtain sensitive data (along with any ways they could try) (Puzas, 2024). Threat that is a way or a method that hacker or attacker use to hack or attack the security of the target. Threat can be virus, but it also can be no virus like DDoS which is sending a lot of packet requests to the server to find the port vulnerability (Seng et al., 2024; Jhanjhi et al., 2021). The literature has extensively examined the security issues related to cloud computing (Humayun et al, 2021). The purpose of this systematic literature review (SLR) is to examine the current body of research on the security, risks, and difficulties of cloud computing (Bader Alouffi, 2021).

 doi:10.20944/preprints202501.0514.v1

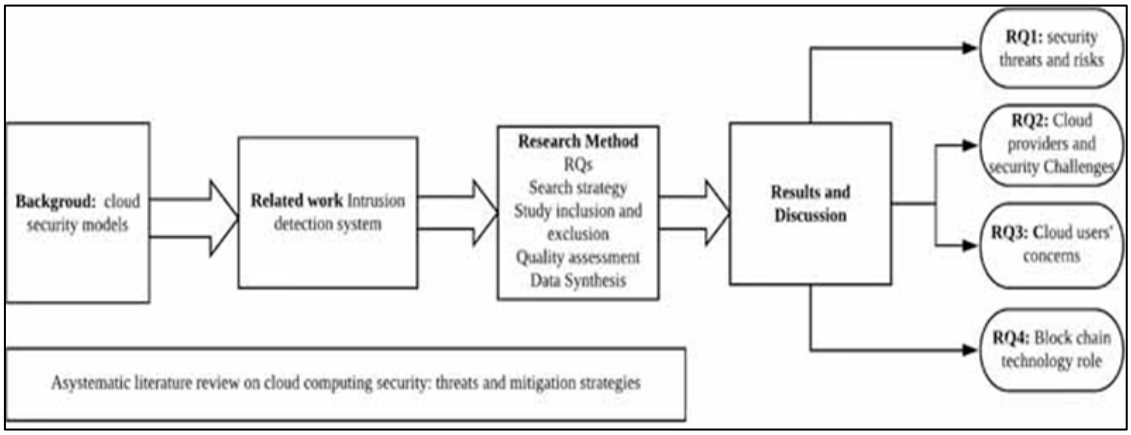

Figure 3. A graphical abstract of systematic literature review on cloud computing.

At a high level, cloud environments face the same threats as traditional data centre environments; the threat landscape is identical (Morrow, 2018). Figure 3 shows a graphical abstract of systematic literature review on cloud computing.

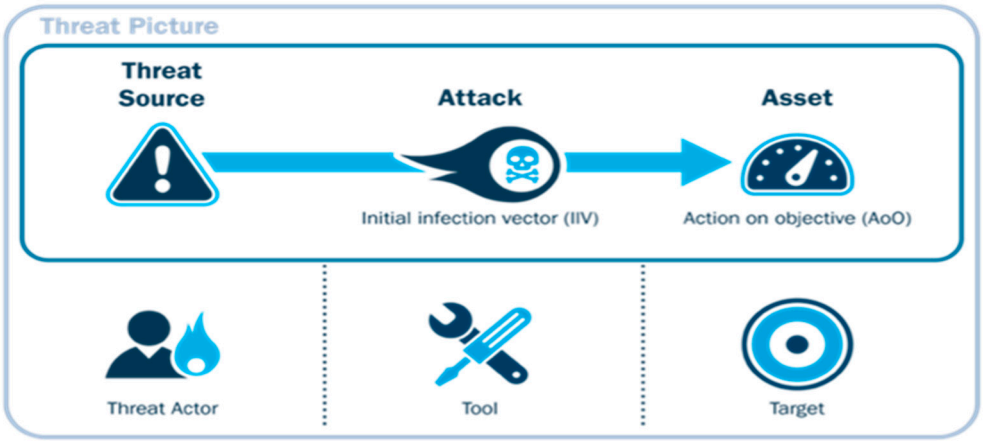

Figure 4. Details of Threats to Cloud Computing Security (Morrow, 2018).

According to the most recent attack surface threat research study from Palo Alto Networks' Unit 42, cloud environments are responsible for four of every five security flaws found in businesses across all industries. 60% of the most prevalent security vulnerabilities listed in this research are caused by web framework takeover (22.8%), remote access services (20.8%), and IT security and networking infrastructure (17.1%) (Ramachandran, 2024). Figure 4 shows details of threats to cloud computing security.

 doi:10.20944/preprints202501.0514.v1

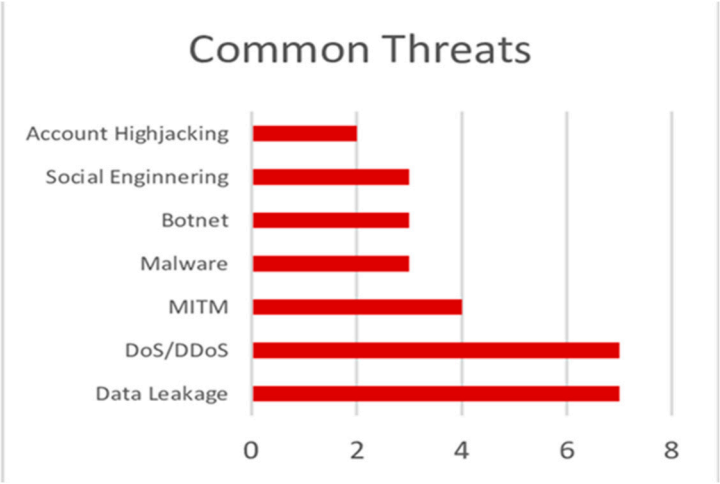

Figure 5. Common Threats to Cloud Computing Security (Alqahtani & Albalawi, 2023).

These typical threats are frequently employed by hackers to breach cloud computing security. After identifying the cloud computing security flaws, they will utilize common attacks to take advantage of the security flaws (Threats, 2024). Figure 5 shows common threats to cloud computing security. We'll go over the common threats it exploits in brief here:

Account Hijacking: When credentials are stolen or authentication is inadequate, a hacker obtains authorized access to user accounts.

Social Engineering: Manipulates human behaviour to gain access to confidential information.

Botnet: Coordinate attacks are carried out by a network of compromised machines.

Malware: Enter cloud systems, corrupt them, or steal data from them.

Man-in-the-Middle (MITM): Steals data by intercepting user and cloud service conversations.

DoS/DDoS: Use packets to overload cloud servers with massive requests to render them inaccessible.

Data Leakage: Sensitive information is exposed to unauthorized parties.

2.4. Example

According to research technologies of cloud security includes Virtual Private Cloud (VPC), Cloud firewall, Identity and Access Management (IAM), and Security Groups, Cloud Monitoring, encryption Data Lost Prevention (DLP), Disaster Recovery and Business Continuity (DR/BC) Planning, Virtual Private Networks (VPNs) and secure APIs and Data Security Posture Management (DSPM).

Firstly, encryption which exist to scramble data until it becomes meaningless. Encryption only allows authorized users to use it, who are in possession of decryption keys. Encryption ensures that data cannot be sold, framed, or used to carry out other non-related actions or attacks without permission or access (Trendmicro, 2020). Following by (IAM), which was its duty for authorizing users (Sindiramutty et al., 2024). The role is about denying access to any suspicious or unauthorized party by assessing a user's identity and privileges, then determines whether the user is allowed access. (IAM) can be said as highly useful in keeping cloud environments secure because no login is attempted (Farber, 2024).

Moreover, cloud firewall. Cloud firewall helps to create a layer which helps to block malicious web traffic such as various malicious bot activity including DDos attacks, vulnerability exploit. The cloud plays an important role in creating a virtual security barrier wrapped around your cloud infrastructure (Tigera, 2021).Fourthly, Virtual Private Cloud (VPC) and Security Groups that provides a full protected and private cloud environment. It controlled in a public cloud whereby it forms out a logically isolated and highly configurable sections of a public cloud. The role of this is to gain access to VPC resources on the increasing of demand as needed by using security groups to

 doi:10.20944/preprints202501.0514.v1

secure your VPC (Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024; Kumar et al., 2021). Each of the security group plays a role as a virtual firewall whereby it allows you to control the outbound and inbound traffic. It can assign with a maximum of five security groups per instance (Tigera, 2021).

Plus, Cloud Monitoring. Cloud monitoring allows review, monitor, and manage your cloud workflow. Besides, it also allows implementation manually and automated cloud monitoring services or tools as needed. Automated monitoring helps in saving time during the working process and ensure continuous visibility. In that sense, administrators will be notified so that a respective mitigation measure can be applied once event occurs so that it helps to ensure the health and secure of the cloud environment (Farber, 2024).

Furthermore, Data Lost Prevention (DLP), which plays a role to detect and prevent potential data breaches through monitoring, identifying, blocking sensitive data from being shared and through accessing inappropriately across cloud services (Farber, 2024). Additionally, Disaster Recovery and Business Continuity (DR/BC) Planning Which helps in ensuring backups, redundancy, and a comprehensive recovery strategy In order to minimize disruptions due to data loss or security incidents (Trendmicro, 2020).Also, Virtual Private Networks (VPNs) and secure APIs that runs to protect data transmission. ESective network segmentation and continuous monitoring of this (VPNs) helps to detect and mitigate risks (Farber, 2024).

Finally, Data Security Posture Management (DSPM) which helps in managing configurations by monitoring data security through identifying risk such as misconfigured access controls or unencrypted data (Tigera, 2021).

3.0. IMPACT

3.1. Benefits

Compared to traditional IT infrastructure, cloud computing has many benefits, especially in terms of flexibility, efficiency, and strategic value. One of the main benefits of the cloud is its flexibility, allowing companies to adjust resources to meet demand and handle varying workloads without paying excessive infrastructure costs. Depending on their security needs and other requirements, companies can also choose between public, private, or hybrid storage options. Cloud providers provide companies the flexibility to choose the level of management they want through a variety of service models, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) (Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024; Lim et al., 2019). Additionally, a wide range of built-in tools allow companies to customize their solutions to their requirements with strong security features such as encryption, virtual private cloud environments, and API keys to protect their data (International Business Machines Corparation, 2024).

Cloud computing improves accessibility in terms of efficiency by making data and apps accessible from any device with an internet connection. Companies can launch products more quickly due to this accessibility, which shortens the time it takes for new applications to get into the market. In addition, cloud storage improves the security of data by using networked backups to protect against data loss due to hardware failures (Sindiramutty et al., 2024; Nayyar et al., 2021). Cloud computing uses remote resources instead of expensive servers and infrastructure can reduce equipment costs. Companies can only pay for the resources they use due to the cloud's pay-as-you-go model, which makes it a cost-effective choice (International Business Machines Corparation, 2024). Through the strategic outsourcing of infrastructure management to cloud providers, cloud computing allows companies to concentrate on their main targets and development. Companies can access the latest technologies without getting to handle maintenance due to frequent updates from cloud providers. Collaboration is also improved by the cloud's globally accessibility, which allows teams to collaborate easily across countries. Lastly, cloud computing gives companies a competitive edge by allowing them to innovate and respond to market developments quickly without concern

 doi:10.20944/preprints202501.0514.v1

about maintaining a large IT infrastructure. Overall, cloud computing is an effective solution for companies looking to innovate, streamline operations, and reduce costs (International Business Machines Corparation, 2024).

3.2. Limitations

Cloud Computing Security not only have benefits, but it also has some limitations and will be discussed as follows:

The first limitation is the bandwidth issues. Users must arrange accordingly and need to avoid crowding many servers and capacity devices into a smaller number of information centres to achieve best performance and efficiency (GeeksforGeeks, 2020). The second limitation is without excess (Sindiramutty, Tan, Shah, et al., 2024). A cloud server is not overabundant or strengthened. Avoid being burned by purchasing an excessive method of action. This is because development can explode to an exceptional level. With any challenge faced, this is often defended since it can lead to additional costs (GeeksforGeeks, 2020).

Other than that, the third limitation is data transfer capacity issues. Users need to prepare for the future and need to avoid constructing huge numbers of servers and storage devices in a small server ranch activity to reach highest performance (GeeksforGeeks, 2020). Furthermore, the fourth limitation is more control. The data and information are transferred when the organization shifts to the cloud (Shah et al., 2022). The organizations that hired in-house IT specialists will not be able to handle problems by themselves. But the cloud service provider will provide a hotline that will be available 24/7 to handle or help to solve the problems (GeeksforGeeks, 2020).

Lastly, the last limitation is no redundancy. There is no extra support for a cloud server. Keeping a cautious distance from getting burned by getting a larger arrangement as the development could often fail. Although there are extra costs needed to be involved, it is usually worthy of it (GeeksforGeeks, 2020).

3.3. Future

The future of cloud computing security will be evolved by the factors of technology and computer environment and most importantly future threats. In this case, here are some of the future paths that cloud computing security might follow:

Firstly, as the quick development of Artificial Intelligence and Machine Learning, the automation of threat detection and response might be one of the futures in the industry. This might be useful for anomaly detection, automation of responding to threats, use predictive analytic models to predict future attacks. This will highly enhance the efficiency and security of Cloud Computing Security.

Secondly, the term “Zero Trust” is becoming a must in cloud computing security. It removes implicit trust, requiring users, devices and applications to do continuous verification. Although it might affect the user experience a little, it brings many security benefits. “Zero Trust” can reduce lateral movement of the threats within the network and help data protection (Sindiramutty, Tan, & Wei, 2024; Sharma et al., 2021). Thirdly, as some organizations are already adopting multi-cloud and hybrid approaches, a unified approach for security is very important. Some tools like Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) are important for constantly maintaining the policies within environments. This strategy helps reduce gaps and enhance monitoring in multi-cloud and hybrid setups.

Lastly, regulatory compliance and data privacy is a main focus for cloud computing security as governments around the globe constantly tighten privacy laws, the cloud security solutions must evolve to keep track of worldwide compliance. In this case, automated compliance reporting and data encryption is a future focus of cloud computing security.

4.0. SECURITY COUNTERMEASURES

 doi:10.20944/preprints202501.0514.v1

Data Leakage:

To prevent data leakage from happening, it is essential to take security countermeasures such as securing all endpoints that are vulnerable to accidental data leakage. An endpoint is responsible for connecting to the network and exchange information with it (Waheed et al., 2024; Singhal et al., 2020). Endpoints can be hard to secure as some organizations have a huge number of connected devices, making it harder to preventing sensitive data from accidentally leaking. In order to solve this matter, organizations should establish a strong and reliable firewall, implement a data loss prevention software into their system and also encrypt all data so that even if a data leakage were to occur, cybercriminals would find it difficult to exploit encrypted data (Kost, 2024).

DoS/DDoS:

One of the most effective ways to prevent DDoS attack is to implement an Anycast network. An Anycast network is responsible for routing incoming traffic to the nearest data center to be processed rather than processing in a single server which can be overwhelmed with traffic. With this network, it can handle traffic spikes by dispersing traffic across multiple servers (CloudFlare, n.d.). Another way to prevent DDoS from happening is to implement rate limiting on cloud servers (CloudFlare, n.d.). This helps prevent cloud servers from being overloaded by limiting the frequency of an activity a user can perform within a certain time (CloudFlare, n.d.).

Botnet:

To prevent a Botnet attack, users should regularly update their systems as system updates can help secure and fix the vulnerabilities present. Another way to prevent botnet attack is to implement multifactor authentication (MFA) as this allows a more secured login environment when accessing websites. This is because by requiring a second form of verification, bots are harder to bypass cloud servers (PingIdentity, n.d.).

Account hijacking:

To prevent cloud account hijacking, users should enforce multifactor authentication (MFA) as this allows users to only access the resources in their cloud accounts after they are done verifying themselves with 2 or more methods. MFA adds an extra layer of protection even if hackers can access the password, they are not able to bypass the additional verification step, which can stop a lot of cloud hijacking activities from occurring (Kasam, 2024).

Malware:

Malware refers to malicious software that is deployed on purpose to intrude the computing environment by exploiting vulnerabilities. One of the countermeasures to deal with malware is malware detection. Malware detection can be categorized into analysis, classification, detection and containment of malware (Wen et al., 2023). Classification techniques are used to categorize malwares according to their instances, which makes new variation to be identified easily based on their type and activities. Malware analysis involves usage of different classification schemes to identify the malware through the features of known malware. Malware detection involves quickly concealing and validating any

instance of malware to exclude further damages to the system. Finally, containment of the virus involves undertaking action to prevent escalation and damages to the system. The next phase will be containment which involves implementing countermeasures to neutralize the malware to prevent any damages to the system (Gounder, 2017).

MITM:

A man-in-the-middle (MITM) attack is a cyberattack performed by the hacker to steal confidential information by eavesdropping on communication between two parties online, such as a user and web application. To prevent MITM attack, the users should only visit the website that uses HTTPS protocol. HTTPS is secured by SSL and TLS protocols, which encrypt the connection between the user's browser and the web server to prevent communication from being eavesdropped. In addition, HTTPS prevents spoofing attacks by authenticating the website with a digital certificate (Gregg Lindemulder, 2024).

 doi:10.20944/preprints202501.0514.v1

Social Engineering:

Social Engineering refers to the act of influencing and manipulating people to divulge sensitive information (Sadiku, 2016). To deal with social engineering attacks, a well written security plan should cover both technical and non-technical approaches that are downward driven by executive management (Alex et al., 2022). This is to ensure that security is integrated into an organization's operational objectives. Moreover, education and training are key components of this policy. The employees should attend awareness campaign about social engineering attacks to prevent them from being targeted by a social engineer (Conteh, 2016).

5.0. PROPOSED COUNTERMEASURES

5.1.1. Enhanced Zero Trust Model

Zero trust is a security model that follows the concept of 'never trust, always verify'. It follows three main principles: Identify, context and security. We proposed to improve this model by adding a few things (Paloalto Networks, n.d.). For once, implement behavioral biometrics in the identification principle to continuously analyse how they interact with devices to prevent any bot activities. For the context principle, enforce the least privilege access by revoking a user's permission after they had completed their task and always validate their identity (Mughal et al, 2024) if they want to access something in the cloud system (Alferidah & Jhanjhi, 2020). For the security principles, implement an adaptive honeypot so that even if an intrusion does happen, it can help confuse and distract the hackers from accessing critical systems by continuously changing their configurations based on the hackers' actions (CloudFlare, n.d.).

5.1.2. AI Enhanced Threats Detection Technologies

AI and ML technologies look for trends and outliers which may occur security breaches. Common supervised learning techniques used for malware and intrusion detection. However, unsupervised learning approaches used to discover unknown dangers through behaviour patterns recognition that is differ from typical system activity in terms of system logs and network traffic (Alkinani et al., 2021). Deep learning (Vijayalakshmi et al., 2021) can be a potential approach for threat identification that utilize neural networks like recurrent neural networks (RNNs) and convolutional neural networks (CNNs) to derive hierarchical features automatically for recognition of sophisticated threats. Furthermore, reinforcement learning can be implemented to facilitate autonomous and adaptive threat response systems that grow and learn from environmental input (Sharma, 2024).

6.0. CONCLUSION

Cloud computing security has become an important aspect of modern technology infrastructure, addressed complex challenges while offered numerous advantages. This report highlights the critical components and threats inherent in cloud environments, such as account hijacking, malware, and data leakage, alongside robust countermeasures like encryption, Identity and Access Management (IAM), and disaster recovery planning. Despite its benefits, such as flexibility and cost-efficiency, cloud security is limited by issues like bandwidth constraints, control deficits, and redundancy challenges.

Emerging trends such as AI-powered threat detection, zero-trust security frameworks, and integrated multi-cloud strategies highlight significant progress in the field. These innovations enable cloud security to better address evolving risks and meet regulatory demands. The report emphasizes the importance of adopting these technologies alongside strategic planning and compliance practices to build secure, adaptable, and robust cloud infrastructures in an increasingly digital landscape.

References

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

Allan Liu, T. Y. (2018). Overview of Cloud Storage. International Journal of Scientific & Technology(1). https://doi.org/hal.science/hal-02889947v1

Alqahtani, K. S., & Albalawi, A. M. (2023). REVIEWING OF CYBERSECURITY THREATS, ATTACKS, AND MITIGATION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT. *Journal of Theoretical and Applied Information*.

https://www.researchgate.net/publication/369897869_REVIEWING_OF_CYBERSECURITY_THREATS_ATTACKS_AND_MITIGATION_TECHNIQUES_IN_CLOUD_COMPUTING_ENVIRONMENT

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

Bader Alouffi, M. H. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. IEEE Access, 9, 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203

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

Chellammal Surianarayanan, P. R. (2023). Cloud Networking. In P. R. Chellammal Surianarayanan, Essentials of Cloud Computing (pp. 105-141). Springer, Cham.

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

 doi:10.20944/preprints202501.0514.v1

CloudFlare. (n.d.). How to prevent DDoS attacks | Methods and tools. CloudFlare: https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

CloudFlare. (n.d.). What is Anycast? | How does Anycast work? CloudFlare: https://www.cloudflare.com/learning/cdn/glossary/anycast-network/

CloudFlare. (n.d.). What is rate limiting? | Rate limiting and bots. CloudFlare: https://www.cloudflare.com/learning/bots/what-is-rate-limiting/

CloudFlare. (n.d.). Zero Trust security | What is a Zero Trust network? CloudFlare: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

Conteh, N. &. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. nternational Journal of Advanced Research in Computer Science, 6(23), 31-38. https://doi.org/10.19101/IJACR.2016.623006

Deyan Chen, H. Z. (2012). Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, 647-651. https://doi.org/10.1109/ICCSEE.2012.193.

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

Fabrizio Marozzo, L. B. (2022). Cloud Computing for Big Data Analysis. Applied Sciences, 12(20). https://doi.org/10.3390/app122010567

Fang Liu, J. T. (2011). NIST Cloud Computing Reference Architecture. NIST Pubs.

Farber, S. (2024, March 6). Cloud Data Security & Protection: Everything You Need to Know. Paloalto Networks: https://www.paloaltonetworks.com/blog/prisma-cloud/cloud-data-security-protection-everything-you-need-to-know/

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

Foster, I. A. (2013, June). *NIST's Security Reference Architecture for the Cloud-First Initiative*. HPC Wire. https://www.hpcwire.com/2013/06/28/nist_s_security_reference_architecture_for_the_cloud-first_initiative/

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

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

Gounder, M. &. (2017). New Ways To Fight Malware. International Journal of Scientific & Technology Research, 6(6), 313-318. https://doi.org/https://www.researchgate.net/publication/317920910_New_Ways_To_Fight_Malware

Gregg Lindemulder, M. K. (2024, June 11). What is a man-in-the-middle (MITM) attack? IBM: https://www.ibm.com/think/topics/man-in-the-middle

 doi:10.20944/preprints202501.0514.v1

Humayun, M., Sujatha, R., Almuayqil, S. N., & Jhanjhi, N. Z. (2022). A Transfer Learning Approach with a Convolutional Neural Network for the Classification of Lung Carcinoma. *Healthcare*, *10*(6), 1058. https://doi.org/10.3390/healthcare10061058

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105-117.

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

International Business Machines Corparation. (2024, August 13). What are the benefits of cloud computing? IBM: https://www.ibm.com/topics/cloud-computing-benefits

International Business Machines Corporation. (2024, August 8). What is a cloud server? IBM: https://www.ibm.com/topics/cloud-server

International Business Machines Corporation. (2024, February 14). Cloud Computing. IBM: https://www.ibm.com/topics/cloud-computing

Jayachander Surbiryala, C. R. (2019). Cloud Computing: History and Overview. 2019 IEEE Cloud Summit, 1-7. https://doi.org/10.1109/CloudSummit47114.2019.00007

Jhanjhi, N., Humayun, M., & Almuayqil, S. N. (2021). Cyber security and privacy issues in industrial internet of things. *Computer Systems Science and Engineering*, *37*(3), 361–380. https://doi.org/10.32604/csse.2021.015206

Jun, A. Y. M., Jinu, B. A., Seng, L. K., Maharaiq, M. H. F. B. Z., Khongsuwan, W., Junn, B. T. K., Hao, A. a. W., & Sindiramutty, S. R. (2024). Exploring the Impact of Crypto-Ransomware on Critical Industries: Case Studies and Solutions. *Preprints.org*. https://doi.org/10.20944/preprints202409.1325.v1

Kasam, A. (2024, March 4). Ways to Prevent Cloud Account Hijacking. ITSecurity Wire: https://itsecuritywire.com/featured/ways-to-prevent-cloud-account-hijacking/

Khalil, I. &. (2014). Cloud Computing Security: A Survey. Computers, 3(1), 1-35. https://doi.org/10.3390/computers3010001

Khan, N. A., Jhanjhi, N. Z., Brohi, S. N., & Nayyar, A. (2020). Chapter Three-Emerging use of UAV's: secure communication protocol issues and challenges, Editor (s): Fadi Al-Turjman, Drones in Smart-Cities.

Kost, E. (2024, November 18). 8 Data Leak Prevention Strategies in 2024. UpGuard: https://www.upguard.com/blog/data-leak-prevention-tips

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

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

Morrow, T. (2018, March 5). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. SEI Blog: https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/

Morrow, T. (2018, March 5). *12 Risks, Threats, & Vulnerabilities in moving to the cloud*. SEI Blog. https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/

 doi:10.20944/preprints202501.0514.v1

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.

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

Nazir, R. &. (2020). Cloud Computing Applications: A Review. EAI Endorsed Transactions on Cloud Systems, 6, 164667. https://doi.org/10.4108/eai.22-5-2020.164667

Paloalto Networks. (n.d.). What is Zero Trust Architecture (ZTA)? Paloalto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

PingIdentity. (n.d.). What Is a Botnet Attack and How to Prevent It. PingIdentity: https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/botnet-attack.html

Puzas, D. (2024, April 1). 12 Cloud Security Issues: Risks, Threats, and Challenges. CrowdStrike: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-risks/

Ramachandran, R. (2024, April 16). Evolving Threats to Cloud Computing Infrastructure and Suggested Countermeasures. ISACA: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/evolving-threats-to-cloud-computing-infrastructure-and-suggested-countermeasures

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

Sadiku, M. &. (2016). Social Engineering: An Introducction. The Journal of Scientific and Engineering Research, 3(3), 64-66. https://doi.org/https://www.researchgate.net/publication/308315268_Social_Engineering_An_Introducction

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

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

Seng, Y. J., Cen, T. Y., Raslan, M. a. H. B. M., Subramaniam, M. R., Xin, L. Y., Kin, S. J., Long, M. S., & Sindiramutty, S. R. (2024). In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations. *Preprints.org*. https://doi.org/10.20944/preprints202408.2261.v1

Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2022). Cybersecurity and blockchain usage in contemporary business. In *Advances in information security, privacy, and ethics book series* (pp. 49–64). https://doi.org/10.4018/978-1-6684-5284-4.ch003

Sharma, R., Singh, A., Kavita, N., Jhanjhi, N. Z., Masud, M., Jaha, E. S., & Verma, S. (2021). Plant disease diagnosis and image classification using deep learning. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *71*(2), 2125–2140. https://doi.org/10.32604/cmc.2022.020017

Sharma, S. K. (2024). AI-Enhanced Cyber Threat Detection and Response Systems. Shodh Sagar Journal of Artificial Intelligence and Machine Learning, 1, 43-48. https://doi.org/10.36676/ssjaiml.v1.i2.14

Shukur, H. &. (2020). Cloud Computing Virtualization of Resources Allocation for Distributed Systems. Journal of Applied Science and Technology Trends, 1(2), 98-105. https://doi.org/10.38094/jastt1331

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

Siva Raja Sindiramutty, H. A. (2023). Innovations in Security: A Study of Cloud Computing and IoT. International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence. https://doi.org/10.54938/ijemdcsai.2023.02.1.252

Threats, T. (2024, May 8). Top Threats to Cloud Computing 2024. ISACA. Cloud Security Alliance: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

Tigera. (2021, December 1). Cloud Security: Challenges and 5 Technologies That Can Help. Tigera: https://www.tigera.io/learn/guides/cloud-security/

Trendmicro. (2020, May 14). Cloud Security: Key Concepts, Threats, and Solutions. Trendmicro: https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions

Vijayalakshmi, B., Ramar, K., Jhanjhi, N. Z., Verma, S., Kaliappan, M., Vijayalakshmi, K., ... & Ghosh, U. (2021). An attention-based deep learning model for traffic flow prediction using spatiotemporal features towards sustainable smart city. *International Journal of Communication Systems*, *34*(3), e4609.

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

Zain Tahir, M. A. (2015). CLOUD COMPUTING INFLUENCE ON OPERATING SYSTEM. SCIENCE INTERNATIONAL.

 doi:10.20944/preprints202501.0514.v1

disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.