IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

Addressing Cloud Computing Security and Visibility Issues

Oluwasanmi Richard Arogundade

Student, Cloud Computing, Campbellsville University, Louisville, United State

Abstract: Network security has become a critical global issue for organizations due to the increasing cyber-attack rate. To enhance organizations' network security, this paper focuses on categorizing the security threat model, which enables examining the impact of threat classes rather than individual impacts. This paper reviews various threat categorization models and proposes criteria for classifying information system security hazards in cloud computing. It also investigates network security vulnerabilities and classifies security concerns using the CIA (confidentiality, integrity, and availability) triangle. Moreover, this paper explains fundamental concepts and procedures for carrying out various network security operations in cloud computing using both paid and open-source tools. This research aims to educate and enable organizations to reduce security threats while having full visibility and control of their infrastructure both in the cloud and on-premises.

Keywords: Network, on-premises, security, cyber-attacks, cloud computing**.**

I. INTRODUCTION

It's crucial to comprehend the cloud concept and architecture before delving into security concerns. Cloud computing has been one of the most significant developments in recent years, enabling individuals and businesses to access computing resources and services over the internet. It is a collection of resources that may be scaled up and down as needed. With little to no interaction with the service provider necessary, it is accessible over the Internet in a "self-service" paradigm. Cloud technology opens up new avenues for the delivery of goods and services in terms of both innovation and affordability. Sharma, & Trivedi, 2014).

Because cloud computing services offer quick access to applications and a decrease in infrastructure expenses, small and medium-sized businesses employ them for a range of functions (Pareek, 2013). Running applications in the cloud has several benefits, including cheaper costs due to pooled computing resources, no upfront infrastructure expenses, and the ability to provision compute resources as needed to meet varying needs. Applications with a high degree of variability in their resource requirements are thus ideally suited to the cloud computing architecture.

The use of virtualization in data centers has been a crucial enabler in making the dynamic provisioning of computer resources a reality. Cloud computing offers several benefits, such as scalability, cost-effectiveness, and flexibility, making it an attractive option for businesses of all sizes. However, cloud computing also poses several security risks, which need to be addressed to ensure confidentiality, integrity, and the availability of cloud services.

II. THE CLOUD CONCEPTS

The cloud concept refers to the delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet. Cloud architecture involves the distribution of computing resources across multiple servers and data centers, allowing for easy access to resources and high availability.

There are four main Cloud deployment models in cloud computing, those deployment model refers to the way in which cloud computing resources are deployed. There are Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud.

2.1 Public Cloud

Public cloud is a cloud computing model in which the infrastructure, such as servers, storage, and applications, is owned and managed by a third-party cloud provider. The resources are shared among multiple organizations over the internet, and users pay only for what they use. Public clouds are highly scalable and cost-effective, making them a popular choice for small and medium-sized businesses. Examples of public cloud providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

Public clouds offer many benefits, such as flexibility, agility, and accessibility. Users can access their resources from anywhere with an internet connection, and they can scale up or down quickly based on their needs. However, public clouds also have some limitations, such as limited customization options and potential security risks due to the shared infrastructure.

2.2 Private Cloud

In a private cloud model, the cloud infrastructure is dedicated to a single organization and is not shared with any other organization. The infrastructure can be managed by the organization itself or by a third-party provider. Private clouds are typically used by organizations with high-security requirements or those that need complete control over their infrastructure.

Private clouds offer many benefits, such as enhanced security, increased control over resources, and greater customization options. Private clouds are often used by government agencies, financial institutions, and healthcare organizations that need to comply with strict regulatory requirements. However, private clouds can be more expensive and less scalable than public clouds.

2.3 Hybrid Cloud

A hybrid cloud model combines the features of public and private clouds. In a hybrid cloud, some of the resources are deployed in a public cloud, while others are deployed in a private cloud. This allows organizations to take advantage of the scalability and cost-effectiveness of the public cloud, while still maintaining control over their sensitive data and applications.

Hybrid clouds offer many benefits, such as flexibility, cost savings, and improved security. Organizations can use the public cloud for non-sensitive workloads and the private cloud for mission-critical applications. However, hybrid clouds can be complex to manage and require a high level of coordination between the public and private cloud environments.

2.4 Community Cloud

Community cloud is a cloud deployment model where a group of organizations with similar requirements share a private cloud infrastructure to achieve common goals like cost savings, resource sharing, or compliance requirements. It offers benefits like improved security, customized services, and better collaboration, but requires a high level of trust and coordination among the participating organizations.

Community clouds are commonly used in industries such as healthcare, finance, education, and government, where multiple organizations need to share resources while maintaining a high level of security and privacy. Community clouds can be managed by one of the participating organizations or by a third-party provider. However, community clouds can be more complex to manage than other cloud deployment models due to the diverse requirements of the participating organizations.

III. CLOUD COMPUTING SERVICE MODELS

Cloud computing service models describe the level of control and responsibility a cloud provider has over the underlying infrastructure and software. Cloud computing has transformed the way businesses operate by providing them with flexible and scalable computing resources, allowing them to focus on their core competencies. Cloud services can be classified into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) - offer varying levels of abstraction and control, allowing businesses to choose the model that best fits their needs.

3.1 IaaS (Infrastructure as a Service)

IaaS is the most basic cloud computing service model, providing virtualized computing resources like servers, storage, and networking infrastructure. This allows businesses to quickly provision and scale resources as needed, without the need for physical infrastructure. The customer retains control over the operating system, middleware, and applications, giving them more flexibility to customize their environment. However, they are still responsible for managing the application, which can be time-consuming and complex.

3.2 PaaS (Platform as a Service)

PaaS, on the other hand, abstracts away the underlying infrastructure, allowing developers to focus solely on building, deploying, and managing their applications. This makes it easier for businesses to quickly develop and deploy

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

applications, without the need for specialized infrastructure knowledge. The cloud provider manages the operating system and infrastructure, which can simplify management and reduce maintenance costs. However, customers have less control over the environment, which may limit their ability to customize and configure the platform.

3.3 SaaS (Software as a Service)

SaaS is the most advanced cloud computing service model, the cloud provider offers a complete software application over the internet. This eliminates the need for businesses to manage the entire stack, from infrastructure to application, and allows them to focus solely on using the software. This model is ideal for businesses that require ready-to-use software applications with minimal setup and maintenance requirements. However, customers have no control over the environment, limiting their ability to customize and configure the software to meet their specific needs.

Cloud computing has revolutionized the way businesses operate, providing access to powerful computing resources without the need for significant upfront investments in hardware and software infrastructure. This has made it possible for small and medium-sized businesses to access advanced technologies that were once only available to larger organizations. By using the cloud, businesses can also reduce their operational costs by paying only for the resources they use and avoiding the need to maintain and upgrade their own hardware and software infrastructure. However, with the benefits of cloud computing come several security risks that must be considered. Cloud providers are responsible for ensuring the security of their infrastructure and services, but customers must also take steps to protect their data and applications. These risks include unauthorized access, data breaches, loss of data, and service outages. To address these risks, businesses must implement appropriate security measures, such as data encryption, access control, and monitoring, and conduct regular security assessments to identify and address vulnerabilities.

IV. PROBLEM STATEMENT

Cloud computing has gained popularity in recent years, more than a third of all enterprise organizations worldwide store data in multiple clouds. The same percentage also keeps data on a private cloud. Having several clouds environment can lead to more entry points for intruders to your infrastructure. Organizations using different cloud environments frequently face the problem of less visibility and more complexity, though the public cloud has its own advantages, including the ability for companies to leverage it for their non-sensitive workloads and their mission-critical workloads in their on-premises IT infrastructure. But it also lacks visibility and adds a lot of complexity to the overall infrastructure. Even if using the cloud can save organizations money in the long run and help them operate more efficiently, it also comes with a number of security dangers for the information and data that is transferred from on-premises to the public cloud. (Behl, 2011). According to Arogundade (2023), the internet is one of the most remarkable inventions in human history, and its contributions to society cannot be overstated. Nevertheless, a negative consequence of this invention is that it has facilitated malicious actors in exploiting weaknesses in computer systems and networks, resulting in data theft, financial losses, and disruption of business operations.

Because of the widespread use of cloud computing, many academics and businesses have begun to weigh in on potential issues that the technology may face. According to a study by Ghanam et al. (2012), security problems were identified as a critical issue in 66 of the research articles assessed. Infrastructure was the second-most important issue at 46, and data management was the third-most important issue at 15. Malicious actors are aiming to take advantage of any new bugs, data sprawl, application sprawl, and potential cloud infrastructure misconfiguration to attack. The impacts of threats or attacks vary greatly; some have an impact on the integrity or secrecy of data, while others have an impact on a system's availability.

The cloud is made up of several technologies with intricately interconnected parts like databases, computer power, networks, etc. Due to the widespread usage of technology, a minor security flaw in a single component might put the entire system to a halt. This variety makes it exceedingly difficult to maintain security in the cloud. Organizations still have trouble understanding the threats to their information assets and how to get the right tools to combat them. The goal of today's cyber-attacks, which come from a variety of sources, is to reveal a company's software and firmware flaws, and rarely are enough time and resources made available for the most important network security, which poses several risks to a network's security. The crucial topic at hand is how to protect our network, both in public and hybrid cloud environments, with more visibility and control.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

V. THE SIGNIFICANCE OF THE STUDY

The significance of this study is twofold. Firstly, it contributes to the growing body of literature on cloud computing security, which is a critical and rapidly evolving field of study. Secondly, it has practical implications for businesses and organizations that are considering adopting cloud computing technologies. By identifying the major security challenges facing cloud computing and proposing mechanisms and solutions to address them, this study can help businesses to make informed decisions about their cloud computing strategy. Specifically, by implementing the recommendations outlined in this study, organizations can reduce the risk of data breaches and cyber-attacks, ensure the confidentiality, integrity, and availability of their data, and maintain regulatory compliance. This, in turn, can help organizations to build trust with their customers, reduce costs associated with data breaches, and improve their overall operational efficiency. Overall, the significance of this study lies in its potential to improve the security posture of organizations that are adopting cloud computing technologies and to foster greater trust in the cloud computing ecosystem

VI. RELATED WORK IN CLOUD COMPUTING SECURITY

Over the past ten years, several research papers have focused on various aspects of cloud computing security challenges. Furthermore, it is evident that most of the papers that were examined and presented did play a significant role in cloud security concerns, and these noteworthy, assessed works were the result of extensive research on this subject that was both perceptive and thorough.

One of the key challenges is the protection of data in transit and at rest. To address this challenge, the use of encryption techniques has been widely advocated. In their study, Sharma et al. (2019) proposed a hybrid encryption technique that combines symmetric and asymmetric encryption to ensure data confidentiality, integrity, and authentication. The proposed technique was evaluated on the Amazon Web Services (AWS) cloud platform, and the results showed that it is effective in securing data in transit and at rest.

Another security challenge in cloud computing is the management of user access and authentication. To address this challenge, several access control models have been proposed. In their study, Singh et al. (2020) proposed a role-based access control (RBAC) model for cloud computing that uses attribute-based encryption (ABE) to ensure data confidentiality.
The proposed model was evaluated on the OpenStack cloud platform, and the results showed that it is effective in managing user access and authentication.

(Mathisen, 2011) examines various important cloud computing security challenges (policy, software, and hardware security), as well as the methods used to lower the risk. According to the author, the use of cloud computing (CC) will rise in the near future. Because more organizations will transfer their data to cloud servers, which will increase the usage of cloud computing (CC), this will also attract a sizable number of hackers. Additionally, he claims that by implementing open standards from the moment CC is adopted, future interoperability and data lock-in issues may be minimized. The author concluded by stating that security is always addressed after cloud computing adoption and that cloud computing still lacks security requirements.

If a company wants to use CC but is hesitant because there aren't adequate standards or procedures in place, it might turn to the Open Cloud Manifesto, the largest open standards movement. Because of how rigid these requirements are, the majority of businesses do not want to adhere to them.

Panth et al. (2014), discuss the defenses used by the most well-known cloud providers against well-known security exploits. In a brief overview of the encryption approaches used in the community, a summary of the security measures used for each cloud provider is provided, with a particular emphasis on the Identity and Access Management (IAM), encryption, and standards utilized by cloud providers.

Bashir and Haider (2011), offer comprehensive research to highlight the cloud computing security issues that are most at risk. This evaluation effort also considers the primary security concerns that cloud providers and their customers have raised in cloud computing by analyzing various security models and solutions.

Kumar et al.(2018), focused on data security concerns, illustrated many types of data security challenges in cloud computing, and provided a strategy for resolving those security difficulties.

Kaur and Singh (2015) A study of security concerns with cloud computing, which presented the challenges surrounding data placement, storage, security, availability, and integrity, has been covered in this study. Although it is important to

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

highlight that the authors merely describe security risks without outlining potential remedies, this evaluation really focuses on one of the significant security concerns.

VII. OVERVIEW OF CLOUD COMPUTING SECURITY

Cloud computing is an innovative technology that provides on-demand access to shared computing resources over the internet. It has gained popularity due to its scalability, flexibility, and cost-effectiveness. However, this technology comes with its own set of security challenges (Sharma & Trivedi, 2014). Security is a major concern in cloud computing due to its multi-tenant nature, where multiple users share a single physical resource, making it difficult to maintain isolation between them. The security of cloud computing is critical because it involves the storage, processing, and transmission of sensitive data.

7.1 Security Concerns in Cloud Computing

Several security concerns exist in cloud computing, which includes data privacy and confidentiality, data integrity, availability, compliance, and regulatory issues (Ghanam et al., 2012). Data privacy and confidentiality are important issues in cloud computing because the data stored in the cloud can be accessible to several users. Data integrity is another critical security concern in cloud computing because data can be corrupted, modified, or deleted by malicious users. Availability is also a major security concern because the cloud is vulnerable to distributed denial-of-service (DDoS) attacks, making it unavailable to legitimate users.

7.2 Classification of Security Concerns

The classification of security concerns in cloud computing is categorized into four broad categories: data security, infrastructure security, application security, and compliance and legal issues (Kaur & Singh, 2015). Data security refers to the protection of data from unauthorized access, data loss, and data leakage (Pareek, 2013). Infrastructure security deals with the security of the cloud infrastructure, including servers, networks, and data centers (Mathisen, 2011). Application security focuses on the security of the applications running on the cloud infrastructure (Bashir & Haider, 2011). Compliance and legal issues relate to regulatory requirements and legal obligations that cloud service providers and users must comply with (Sharma & Trivedi, 2014).

7.3 Fundamental Concepts and Procedures for Network Security Operations

Fundamental concepts and procedures for network security operations in cloud computing include using a multi-layered approach to security, implementing strict access controls, encrypting data, and implementing intrusion detection and prevention systems (IDPS) (Niklas Krumm, 2023). The use of firewalls and VPNs can also help protect the cloud infrastructure from unauthorized access (Panth et al., 2014). Additionally, continuous monitoring and auditing of the cloud infrastructure can help identify and mitigate security threats in a timely manner (Ghanam et al., 2012).

7.4 Threat categorization models

Threat categorization models are useful for classifying security threats and understanding their impact on information systems over time. According to Hashizume et al. (2013), the majority of threat categorization models classify security threats based on the following dimensions:

- Attack location: where the threat is coming from
- Attack target: what the threat is targeting
- Attack method: how the threat is carried out
- Attack motivation: why the threat is being carried out
- Attack impact: what the consequences of the threat are

Other researchers have proposed alternative models. For instance, Ghanam et al. (2012) propose a hybrid approach that combines the STRIDE model and the DREAD model. The STRIDE model classifies threats based on six categories: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The DREAD model assesses the severity of a threat based on five categories: damage potential, reproducibility, exploitability, affected users, and discoverability. Kshetri (2013) proposes an institutional evolution framework for understanding privacy and security issues in cloud computing. This framework identifies four stages of institutional evolution: initiation, expansion, maturity, and decline. At each stage, different security threats may arise and different institutional responses may be required. Regardless of the specific model used, threat categorization can help organizations prioritize security measures and develop more effective risk management strategies. By understanding the types of threats that are most likely to occur and their potential impact, organizations can allocate their resources more effectively and take proactive steps to mitigate security risks.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

VIII. NETWORK SECURITY VULNERABILITIES

Network security vulnerabilities are a major concern in cloud computing because the cloud relies heavily on the internet for communication between different components. Some of the network security vulnerabilities include data interception, eavesdropping, and man-in-the-middle attacks (Wieder & Yahyapour, 2013). Data interception occurs when an attacker intercepts the communication between the cloud service provider and the user. Eavesdropping is the unauthorized monitoring of network traffic, while man-in-the-middle attacks occur when an attacker intercepts the communication between two parties and modifies the data before forwarding it to the intended recipient. The shared nature of cloud computing resources also poses a risk, as VMs from different users may be hosted on the same physical server, making it possible for an attacker to access other users' data through a compromised VM (Kumar et al., 2018). Network security vulnerabilities can also arise due to the use of outdated software, unpatched systems, and the lack of proper access controls (Huang et al., 2023).

8.1 Criteria for classifying information system security hazards in the cloud

Cloud computing presents unique security challenges due to its shared infrastructure, distributed environment, and dynamic nature. Therefore, we propose criteria for classifying information system security hazards in cloud computing, including:

- Attack Vector: This criterion identifies the method used by attackers to compromise the system, such as network-based attacks, application-based attacks, or physical attacks.
- Attack Type: This criterion identifies the type of attack, such as denial-of-service attacks, data-breaches, or malware attacks.
- Impact Level: This criterion identifies the level of impact of the attack on the organization, such as low, medium, or high.
- Target Asset: This criterion identifies the asset targeted by the attacker, such as data, applications, or infrastructure.

8. 2. Network security vulnerabilities and the CIA Triangle

Network security vulnerabilities can be classified based on the CIA (confidentiality, integrity, and availability) triangle. Confidentiality refers to ensuring that data is only accessible by authorized individuals or systems. Integrity refers to ensuring that data is accurate and unmodified. Availability refers to ensuring that data and services are available and accessible when needed. Network security vulnerabilities can impact one or more elements of the CIA triangle. Some common network security vulnerabilities include:

- Malware:
- Malware refers to any software designed to harm or exploit a system. Malware can compromise the confidentiality, integrity, and availability of data and services.
- Phishing:
- Phishing refers to the practice of tricking users into revealing sensitive information, such as passwords or credit card numbers. Phishing attacks can compromise the confidentiality and integrity of data.
- Denial of Service (DoS):
- DoS attacks aim to disrupt the availability of services by overwhelming them with traffic or requests. DoS attacks can compromise the availability of services.
- Ransomware:
- Ransomware is a type of malware that encrypts data on a system and demands a ransom payment in exchange for the decryption key. Ransomware attacks can compromise the confidentiality and availability of data.
- Man-in-the-Middle (MitM) attacks:
- MitM attacks occur when an attacker intercepts communication between two parties, allowing them to eavesdrop on or modify the communication. MitM attacks can compromise the confidentiality and integrity of data.
- Cross-Site Scripting (XSS):
- XSS attacks occur when an attacker injects malicious code into a web page, allowing them to execute arbitrary code in the victim's browser. XSS attacks can compromise the confidentiality and integrity of data. SQL Injection: SQL injection attacks occur when an attacker injects malicious SQL code into a database query, allowing them to execute arbitrary commands or steal data from the database. SQL injection attacks can compromise the confidentiality and integrity of data.
- Insider threats

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

- Insider threats refer to threats posed by employees or other trusted insiders who have access to sensitive data or systems. Insider threats can compromise the confidentiality, integrity, and availability of data and services.
- Zero-day exploits
- Zero-day exploits refer to vulnerabilities in software or systems that are unknown to the vendor or developer. Zero-day exploits can be used by attackers to gain unauthorized access to systems or steal sensitive data.

IX. THE PROPOSED APPROACHES FOR SECURITY AND VISIBILITY ISSUES

Based on the literature review, there are several solutions that can be adopted to address cloud computing security and visibility issues. These include:

9.1 Implementing Multi-Factor Authentication (MFA)

MFA is a security mechanism that requires users to provide two or more forms of authentication to access a system. This can include something the user knows (e.g., a password), something the user has (e.g., a smart card), and/or something the user is (e.g., a fingerprint). The concept involves users presenting a mixture of authenticator codes in order to confirm their identity prior to gaining entry to their accounts or servers on your network or systems (Arogundade, 2023).

By implementing MFA, organizations can reduce the risk of unauthorized access to their cloud computing systems and data. Multi-Factor Authentication (MFA) is an effective security measure that can significantly reduce the risk of unauthorized access to cloud computing systems and data. MFA requires users to provide two or more forms of authentication, adding an extra layer of security beyond the traditional username and password. This approach helps to prevent unauthorized access even if a password is compromised. MFA is a security mechanism that requires users to provide two or more forms of authentication to access a system. It can include something the user knows (e.g., a password), something the user has (e.g., a smart card), and/or something the user is (e.g., a fingerprint) (Ibrokhimov et al., 2019). MFA is an essential component of cloud security as it helps to reduce the risk of unauthorized access to cloud computing systems and data (Ogbanufe & Baham, 2022).

Implementing MFA is relatively easy and can be done through various methods, such as integrating MFA into existing authentication systems or using cloud-based MFA solutions. Cloud providers often offer MFA solutions that can be easily integrated with their platforms, allowing organizations to add an extra layer of security to their cloud systems without having to manage the underlying infrastructure. Studies have shown that MFA can significantly improve the security of online accounts and systems (Das et al., 2019). However, user perceptions and mental models of MFA can influence its adoption and effectiveness (Das et al., 2020). In addition, the use of MFA with a smart card and fingerprint has been proposed as a secure method for access control in various applications, including parking gates (Insan et al., 2019).

9.2 Encryption

Encryption is the process of converting data into a coded language to prevent unauthorized access. Encryption is a critical security measure that can protect sensitive data in transit and at rest in the cloud. Encrypting data before it is transmitted to the cloud can help prevent unauthorized access and protect against data breaches. Encryption works by converting data into a coded language using a mathematical algorithm, making it unreadable to anyone who does not have the encryption key. Cloud providers offer various encryption options to help organizations secure their data in the cloud. For instance, Amazon Web Services (AWS) provides the option to encrypt data both in transit and at rest using a range of encryption algorithms, including Advanced Encryption Standard (AES) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols. Similarly, Microsoft Azure offers encryption options for both data in transit and at rest using Azure Storage Service Encryption (SSE) and Transport Layer Security (TLS) protocols.

Encryption is a crucial security measure for protecting data in the cloud, and there are various encryption algorithms and techniques available to organizations. One example is an identity-based encryption (IBE) algorithm, which uses a recipient's identity (such as an email address) as the public key for encrypting data, making it easier to manage and distribute encryption keys (Cao et al., 2021). Another study discusses the role of encryption in democratic practices in the digital era and emphasizes the importance of encryption in protecting individual privacy and freedom of speech (Monsees, 2019). In addition to IBE, there are also various encryption algorithms available for color images, such as the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) (Ghadirli et al., 2019). Furthermore, a review and evaluation study of symmetric encryption algorithms highlights the importance of selecting the appropriate encryption algorithm based on the specific use case and security requirements (Alenezi et al., 2020). In summary, encryption is a vital security measure for cloud computing, and organizations should carefully consider the encryption algorithms and techniques best suited for their specific needs.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

9.3 Network Segmentation

Network segmentation is a critical security measure that involves dividing a network into smaller, more secure subnetworks. This approach can effectively reduce the attack surface and limit the scope of potential security breaches or attacks. By segmenting a cloud network, organizations can effectively isolate specific systems or applications, limiting their exposure to potential security threats. Cloud providers offer various tools and services that allow organizations to segment their cloud networks. For instance, virtual private clouds (VPCs) are private networks that organizations can create within a public cloud environment. VPCs provide a high degree of isolation and control, allowing organizations to define their own virtual network topology and IP address range. Organizations can also use access control lists (ACLs) and security groups to restrict traffic between VPCs and prevent unauthorized access to critical resources.

In addition to VPCs, organizations can also use software-defined networking (SDN) technologies to implement network segmentation in the cloud. SDN enables network administrators to manage network traffic and security policies through a centralized controller, providing greater visibility and control over network traffic (Kumar & Shenoy, 2018). SDN also allows organizations to enforce policy-based segmentation, which automatically segments traffic based on predefined policies. Network segmentation is a critical security measure that can help organizations reduce the impact of potential security incidents in the cloud. By segmenting their networks and restricting access to critical resources, organizations can effectively limit the scope of potential attacks and improve their overall security posture in the cloud.

9.4 Continuous Monitoring

Continuous monitoring involves the real-time monitoring of a system to identify and respond to security threats as they occur. Continuous monitoring is a critical component of cloud security, as it allows organizations to identify and respond to security threats in real-time. As noted by Kaur and Singh (2015), continuous monitoring enables organizations to "detect anomalous activities or suspicious behavior and respond to security incidents in a timely manner." This is particularly important in cloud environments, where the dynamic nature of the infrastructure can make it challenging to detect and respond to security incidents.

According to Hashizume et al. (2013), continuous monitoring is an essential security practice in cloud computing, as it enables organizations to "monitor the security posture of their cloud infrastructure, including the network, servers, applications, and data." This allows organizations to identify potential security vulnerabilities and respond quickly to any security incidents that may occur. Continuous monitoring can be implemented using a variety of tools and technologies, including intrusion detection and prevention systems, log analysis tools, and security information and event management (SIEM) solutions (Kumar et al., 2018). By leveraging these tools, organizations can gain real-time visibility into their cloud infrastructure and identify and respond to security threats as they occur. continuous monitoring is a critical security practice in cloud computing, as it enables organizations to detect and respond to security incidents in real time, reducing the potential impact of these incidents on their infrastructure and data.

9.5 More Visibility with less Complexity

The idea of hybrid clouds is gaining popularity among organizations running multiple cloud environments. This approach allows businesses to use the public cloud while maintaining key components of their on-premises IT systems. However, implementing a hybrid cloud can be complex and expensive to manage, and gaining visibility into the infrastructure can be challenging. End-to-end visibility is crucial to success in a hybrid context, and individualized dashboards and filters can help achieve this. Cloud providers offer services to create dashboards with real-time visibility, such as AWS CloudWatch. Detailed insights into how data moves across various stages of business processes are also important. Tools like AWS X-ray can aid in the analysis and debugging of distributed applications for developers. To maximize the effectiveness of a hybrid deployment, IT teams should look for important characteristics in a hybrid monitoring platform beyond just performance charts. (Mok et al., 2021; Krishnan & Gonzalez, 2015)

9.6 Cloud Access Security Brokers (CASBs)

Cloud Access Security Brokers (CASBs) are becoming an increasingly popular solution for securing cloud infrastructure. They act as a gatekeeper between an organization's on-premises infrastructure and cloud service providers, allowing administrators to extend their security policies into cloud environments. By providing a centralized point of control, CASBs can enforce security policies consistently across multiple cloud services. Cloud Access Security Brokers (CASBs) have emerged as a crucial security solution for organizations that use cloud computing services. According to a report by Gartner, "by 2023, 60% of large enterprises will use a CASB to govern cloud services, up from less than 20% in 2018" (Gartner, 2020)

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

One of the key features of CASBs is their ability to provide identity and access management (IAM) capabilities. This includes features such as single sign-on (SSO), multi-factor authentication (MFA), and role-based access control (RBAC), which help organizations control who has access to their cloud resources. CASBs can also provide real-time visibility into user activity, allowing organizations to monitor cloud usage and detect anomalous behavior.
Another important feature of CASBs is their data loss prevention (DLP) capabilities. These features help prevent the unauthorized sharing of sensitive data by identifying and blocking attempts to upload or download sensitive information. CASBs can also encrypt data at rest and in transit, providing additional protection for sensitive data.
CASBs are available as cloud-based or on-premises solutions, depending on an organization's needs. Cloud-based CASBs offer greater scalability and ease of management, while on-premises solutions provide more control over data and configuration. Ultimately, the choice of which type of CASB to implement depends on an organization's specific requirements and security needs.

CASBs provide a powerful set of tools for securing cloud infrastructure. By providing visibility into cloud usage, enforcing security policies, and protecting sensitive data, they help organizations maintain a strong security posture in the cloud. As such, CASBs are expected to continue to gain popularity in the coming years as more organizations adopt cloud services.

9.7 Configuration management and auditing

When shifting workloads to the cloud, compliance, and security considerations are crucial. Configuration management and auditing can help lower security concerns. Advanced hybrid cloud visibility technologies can monitor vulnerabilities and configuration changes, and proactively audit network ACLs and route tables. Flow logs can be used to compare and identify aberrant activities and generate alarms. A set of tools native to the cloud is necessary for network visibility in the cloud. here is a brief overview of how to develop a thorough cloud network visibility program.
visibility program.

- Conduct an assessment of your current network monitoring resources to identify strengths and weaknesses.
- Choose tools that support both on-premises and cloud environments and allow for centralized management.
- Connect network subnets and virtual private clouds (VPCs) to achieve optimal network scalability and design.
- Monitor network traffic by gathering flow information for workloads within network segments and subnets (e.g., VPC flow logs).
- Maximize security by leveraging security groups and other network access restrictions and keeping logs of relevant events.
- Capture network packets, send them to a centralized network visibility and analytics system, and filter out those that are not needed for monitoring or security purposes.
- Record and analyze network traffic and information using a dedicated network visibility tool.

X. CONCLUSION AND RECOMMENDATIONS

The advantages of cloud computing include rapid system implementation, low costs, abundant storage, and simple system access from anywhere at any time. Therefore, cloud computing is a clearly emerging technology that is a commonly used computer environment globally. However, there are several security and privacy issues that make the use of cloud computing difficult. The vulnerabilities, risks, and attacks that exist in the cloud should be properly understood by all users of the cloud. This study focused on analyzing the security threats and vulnerabilities in cloud computing and providing recommendations to mitigate these threats. The analysis of the security threat model revealed that cloud computing faces a wide range of threats, such as data breaches, denial-of-service attacks, and insider attacks. Network security vulnerabilities were also identified, such as insecure APIs and poor network design, that could be exploited by attackers.

Furthermore, the classification of security concerns in cloud computing showed that data security, privacy, and compliance were major concerns for organizations using cloud services. The study also discussed fundamental concepts and procedures for network security operations in cloud computing, emphasizing the importance of access control, data encryption, and regular security assessments.

10.1 Implications of the study

The study highlights the importance of understanding and addressing security threats and vulnerabilities in cloud computing. The findings have implications for organizations using cloud services, as they need to ensure the security of

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10321

their data and applications in the cloud. The study provides recommendations to help organizations mitigate security risks and maintain their data's confidentiality, integrity, and availability.

10. 2. Limitations of the Study

One of the limitations of this study is its scope, which focused on analyzing security threats and vulnerabilities in cloud computing. Further research could explore other aspects of cloud computing security, such as regulatory compliance, legal issues, and service-level agreements.

3.Future Research Directions

Future research could explore emerging threats and vulnerabilities in cloud computing, such as machine learning-based attacks and quantum computing attacks. Additionally, the research could focus on developing more advanced security solutions for cloud computing, such as using blockchain technology to enhance data security and privacy.

10.4 Recommendations for Organizations Using Cloud Computing Services

Based on the findings of this study, organizations using cloud computing services should:

- Conduct regular security assessments and audits to identify vulnerabilities and mitigate security risks.
- Implement strong access control measures to limit the exposure of sensitive data and applications.
- Use data encryption to protect data at rest and in transit.
- Ensure compliance with relevant regulations and standards, such as General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).
- Monitor network activity and logs for suspicious behavior and indicators of compromise.
- Choose a reputable cloud service provider (CSP) that offers robust security measures and provides transparency into their security practices.
- Establish a comprehensive security policy that outlines roles, responsibilities, and procedures for maintaining the security of cloud computing services.
- Train employees on cloud security best practices and raise awareness about common security threats and vulnerabilities.
- Implement multi-factor authentication (MFA) to add an extra layer of security to user logins and access.
- Regularly patch and update cloud systems and applications to address known vulnerabilities and reduce the risk of exploitation.
- Perform regular backups of critical data to ensure business continuity in the event of a security incident or data loss.
- Conduct regular incident response drills and develop a response plan in the event of a security incident.
  It's important for organizations to continuously assess and evaluate their security posture to ensure that their cloud computing services remain secure and compliant with industry standards and regulations. By adopting a proactive approach to cloud security, organizations can minimize the risk of security incidents and protect their sensitive data and applications from cyber threats.

REFERENCES

[1]. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[2]. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[3]. Arogundade, O. R. (2023). Network Security Concepts, Dangers, and Defense Best Practical. Computer Engineering and Intelligent Systems, Vol.14, No.2, 2023, (ISSN 2222-2863). https://doi.org/10.7176/CEIS/14-2-03

[4]. Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. (2021). IIBE: an improved identity-based encryption algorithm for WSN security. Security and Communication Networks, 2021, 1-8.

[5]. Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating user perception of multi-factor authentication: A systematic review. arXiv preprint arXiv:1908.05901.

[6]. Das, S., Wang, B., Kim, A., & Camp, L. J. (2020). Mfa is a necessary chore!: Exploring user mental models of multi-factor authentication technologies.

[7]. Monsees, L. (2019). Crypto-politics: Encryption and democratic practices in the digital era. Routledge.

[8]. Ghanam, Y., Ferreira, J., & Maurer, F. (2012). Emerging Issues & Challenges in Cloud Computing—A Hybrid Approach. Journal of Software Engineering and Applications, 05(11), 923–937. https://doi.org/10.4236/jsea.2012.531107

DOI: 10.17148/IARJSET.2023.10321

[9]. Ghadirli, H. M., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. Signal Processing, 164, 163-185.

[10]. Gartner. (2020). Critical Capabilities for Cloud Access Security Brokers.

[11]. Goudreault, S. (2022, November 2). Definitive Guide to Hybrid Clouds, Chapter 3: Understanding Network Visibility in the Hybrid Cloud. Gigamon Blog. https://blog.gigamon.com/2022/11/02/definitive-guide-to-hybrid-clouds-chapter-3-understanding-network-visibility-in-the-hybrid-cloud/

[12]. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5. https://doi.org/10.1186/1869-0238-4-5

[13]. Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., & Sain, M. (2019, February). Multi-factor authentication in cyber physical system: A state of art survey. In 2019 21st international conference on advanced communication technology (ICACT) (pp. 279-284). IEEE.

[14]. Insan, I. M., Sukarno, P., & Yasirandi, R. (2019). Multi-factor authentication using a smart card and fingerprint (case study: Parking gate). Indonesia Journal on Computing (Indo-JC), 4(2), 55-66.

[15]. kaur, M., & Singh, H. (2015). A Review of Cloud Computing Security Issues. International Journal of Education and Management Engineering, 5(5), 32–41. https://doi.org/10.5815/ijeme.2015.05.04

[16]. Krishnan, S. P. T., & Gonzalez, J. L. U. (2015). The Google Cloud Platform Difference. In Building Your Next Big Thing with Google Cloud Platform (pp. 3-12). Apress, Berkeley, CA. DOI: 10.13005/ojcst11.04.02

[17]. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science, 125, 691–697. https://doi.org/10.1016/j.procs.2017.12.089

[18]. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37 (4–5), 372–386. https://doi.org/10.1016/j.telpol.2012.04.011

[19]. Ogbanufe, O. M., & Baham, C. (2022). Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. Information Systems Frontiers, 1-20.

[20]. Pareek, P. (2013). Cloud Computing Security from Single to Multi-Clouds using Secret Sharing Algorithm. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET).

[21]. Panth, D., Mehta, D., & Shelgaonkar, R. (2014). A Survey on Security Mechanisms of Leading Cloud Service Providers. International Journal of Computer Applications, 98(1), 34–37. https://doi.org/10.5120/17149-7184

[22]. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 199-212).

[23]. Shaikh, F. B., & Haider, S. (2011). Security threats in cloud computing. International Conference for Internet Technology and Secured Transactions, 214–219. http://fs3.dajie.com/2012/08/13/031/13448264310678702.pdf

[24]. Sharma, R., & Trivedi, R. K. (2014). Literature review: Cloud Computing –Security Issues, Solution and Technologies. International Journal of Engineering Research, 3(4), 221–225. https://doi.org/10.17950/ijer/v3s4/408

[25]. Srinivasan, S., & Poornima, R. (2014). Security issues in cloud computing—a survey of risks, threats and vulnerabilities. Procedia Engineering, 97, 2114-2120.

[26]. Mathisen, E. (2011). Security challenges and solutions in cloud computing. IEEE International Conference on Digital Ecosystems and Technologies. https://doi.org/10.1109/dest.2011.5936627Bashir SF, Haider S (Dec 2011) Security threats in cloud computing. In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214–219

[27]. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

[28]. Mok, R. K., Zou, H., Yang, R., Koch, T., Katz-Bassett, E., & Claffy, K. C. (2021, November). Measuring the network performance of Google Cloud platform. In Proceedings of the 21st ACM Internet Measurement Conference (pp. 54-61).

