ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep164

Review on Information Security Risk and Control Measures Based on Cloud Computing Environment

Abdulrahman Malik Haji[1]; Suleiman Abdalla Baho[2]

[1]School of Computer Science Communication and Media Studies the State University of Zanzibar
[2]School of Business the State University of Zanzibar

Publication Date: 2025/09/11

Abstract: The high cost of data security breaches raises the reputation of information security for all information users. Public and governmental organizations that offer information services to citizens must protect their services and train their employees to safeguard their information assets. To ensure the stability and efficiency of the data services, several users and organizations are shifting their services to cloud environments. Cloud computing provides services to users including Software as Services (SaaS), Infrastructure as a Services (IaaS), and Platform as a services (PaaS) with high degree of data confidentiality, integrity, and availability but observation show that there is a major problem of data leaking and attacks on the organization setup which therefore hindering the effectiveness of cloud services among users. This paper reviews the potential risks related to cloud computing and determines control measures to overcome the data privacy issue based on the general and architectural cloud environment.

Keywords: *Cloud Computing, Cloud Attacks, Security Architecture, Shared Responsibility Model.*

How to Cite: Abdulrahman Malik Haji; Suleiman Abdalla Baho (2025) Review on Information Security Risk and Control Measures Based on Cloud Computing Environment. *International Journal of Innovative Science and Research Technology*, 10(9), 269-274. https://doi.org/10.38124/ijisrt/25sep164

I. INTRODUCTION

Information security aspects such as data confidentiality, integrity, and availability are essential security components in cloud computing technology [1]. Data protection is a concern when moving data into or out of the cloud, as well as when the data is stored. Issues like data damage, unauthorized modifications, and impersonation are common challenges that cloud providers must address to build trust with users regarding data safety. Therefore, this storage should be a shared responsibility between the cloud provider and the user by ensuring privacy and data integrity. In traditional data security, various methods were used to process and protect sensitive data. To secure data that is stored externally, encryption is a commonly used method for data protection [2]. As the need to store data continues to grow, traditional security methods are becoming less effective. The provider manages critical and sensitive customer data, but this does not always ensure data integrity, privacy, and user trust [3].

II. THE CONCEPT OF CLOUD COMPUTING

As addressed by [20], cloud computing is a technological methods allow users to access shared computing resources and services over the internet, from anywhere in the world, using compatible devices like laptops, smartphones, and tablets. Key features identified include internet accessibility, resource flexibility, multi-tenancy, and self-service configuration. Various studies [21-22] have highlighted the three main service models of cloud environments, which are:

- SaaS provides software applications that can be accessed via the internet, reducing the need for local installation and maintenance.
- PaaS offers a cloud-based platform that includes everything developers need to build, test, deploy, and manage applications, such as operating systems, development tools, database management, and middleware. Examples of such platforms include Google App Engine, Microsoft Azure App Service, and Heroku, among others.
- IaaS provides virtualized hardware resources such as servers, storage, and networking devices, offering full control over operating systems and applications.

III. AN OVERVIEW OF CIA BASED ON CLOUD COMPUTING

The three core aspects of information security including confidentiality, integrity, and availability (CIA)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep164

define an organization's approach to security. All information security controls, measures, threats, vulnerabilities, and processes are governed by the CIA standard [4].

➢ *Confidentiality*

Confidentiality refers to preventing the intentional or unintentional unauthorized release of information. The loss of confidentiality can occur through various means, such as the deliberate disclosure of confidential information by an organization or the improper use of network privileges. To ensure privacy, several fundamental techniques are employed, including network security protocols, network authentication services, and data encryption services. The work of [17] examined the CIA triad (confidentiality, integrity, availability), and it was emphasized that confidentiality depends on authentication, data encryption, firewalls, and antivirus solutions.

➢ *Integrity*

Integrity ensures that the message sent is the same message received and that it is not altered either intentionally or unintentionally. The loss of integrity can occur due to planned attacks aimed at changing information [2, 5]. Integrity also involves the concept of non-repudiation, which means the sender cannot deny having sent a message. To maintain integrity, certain principles are applied, such as firewall services, communication security management, and intrusion detection services.

➢ *Availability*

This terminology refers to ensuring reliability and stability in cloud systems. It guarantees that connectivity is accessible when required, allowing authorized users to access the network or systems. According to [18], availability is identified as the frequency with which a cloud service is accessible and operational when required, and it underscores the importance of fault tolerance through redundancy or replication across instances, as well as the significance of network reachability. The research in [19] suggested that principles such as acceptable login procedures, operating process performance, reliable and interoperable security processes, network security mechanisms, and fault tolerance for data availability—such as backups and redundant disk systems—are used to ensure availability.

IV. THE COMMON ATTACKS TO THE CLOUD ENVIRONMENT

This section outlines the most common threats that target cloud resources. The author of [7, 8, 6] categorized these threats into the following groups:

➢ *Weak Identity and Access Control*

User credentials and access control are crucial for the security of cloud resources. Poor identity and access control can lead to the following:

- Logon Abuse: If cloud broker console or API credentials are compromised, this type of abuse mainly targets users who may be legitimate users of another system or users with lower security clearance. This can enable malicious actors outside the organization to take control of the cloud environment.
- Information Breaks: Weak access controls on computing services and data storage can result in the exposure of sensitive information, which has been a major cause of data breaches in cloud environments.
- Malware Insiders: Malicious insiders attempting to gain administrative access and privileges can cause damage to sensitive data and the network.
- Abuse and Notorious Use of Cloud Services: Account hijacking of a cloud account can allow a malicious user to misuse the allocated resources for activities such as launching DDoS attacks, sending spam, and conducting phishing operations, leaving the organization vulnerable to legal issues.

➢ *Network Attack*

DoS and DDoS attacks: Inadequate network isolation and firewall management can expose cloud services to DoS and DDoS attacks, which can degrade cloud application performance and even cause service outages. DoS attacks may use the following methods to consume a target's resources:

- Filling up a target's hard drive storage space using large email attachments or file transfers.
- Sending messages that reset a target host's subnet mask, thereby disrupting the target's network operations.
- Exhausting a target's resources to accept network connections can lead to new connections being refused.

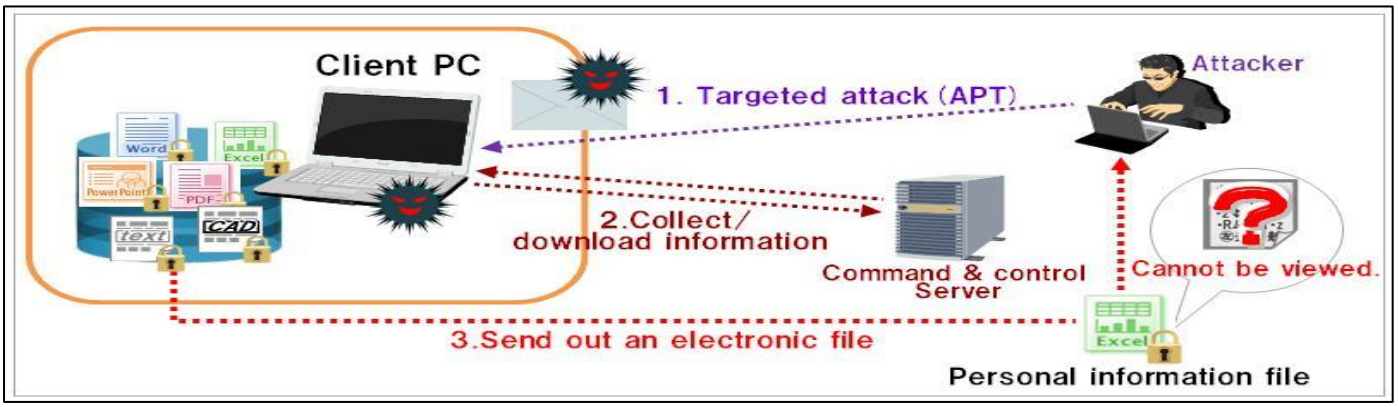

Fig 1 How an Attacker Interrupts a Network Service

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep164

➢ *Workload Threats*

- Advanced Persistent Threats (APTs): Malware and APTs, once inside an environment, adjust to security controls and gradually establish a presence. They move laterally within the network and, upon reaching their objectives, identify and exploit vulnerabilities.
- Vulnerabilities: Since cloud services support multiple users, weaknesses like privilege escalation and virtual machine boundary breaches can lead to data leaks and expose applications and workloads.
- Insecure Application Services: APIs that are not secured properly can make different parts of an application vulnerable to common attacks, causing service interruptions or data breaches.

Fig 2 Advanced Persistent Threats (APTs)

➢ *Inappropriate System use*

This kind of network attack involves authorized users using the network for personal purposes, such as visiting websites with inappropriate content like travel, pornography, or sports sites [8]. According to the International Information Systems Security Certification Consortium (ISC) Code of Ethics and the Internet Advisory Board (IAB), Recommendations using networked services for non-business reasons may be viewed as system misuse. Although most employers do not enforce very strict web usage policies, there could be occasional legal issues if employees access pornographic sites or run their own online businesses using company resources.

➢ *Back-Door*

A back-door attack occurs through dial-up modems or other external connections. The attacker gains access to a network by bypassing security measures and entering through a back door, such as a modem [9].

➢ *TCP Hijacking*

In this attack, an attacker takes over a session between a trusted client and a server. The attacker replaces the client's IP address with their own, and the server continues the communication, believing it is interacting with the trusted client.

➢ *Social Engineering*

This attack uses social techniques to get sensitive information, such as passwords or PINs, for use against cloud systems [5, 10]. For instance, an attacker may pretend to be someone from an organization and call employees to request passwords for maintenance purposes. Some additional examples of social engineering attacks include:

- E-mails sent to employees by attackers asking for passwords to verify the organizational database after a network breach.
- E-mails sent to employees by attackers requesting passwords because work needs to be done on the system over the weekend.
- E-mails or phone calls from attackers who pose as officials investigating. and ask for passwords.
- Sharing medical information with individuals pretending to be doctors and asking for patient records.

V. SECURITY ARCHITECTURE IN A CLOUD ENVIRONMENT

Security architecture in cloud computing plays a crucial role in building trust in the cloud model.

As mentioned in [23], techniques like self-management and access control are essential for creating a secure environment, protecting cloud storage, and supporting microarchitectures. Additionally, an autonomic computing architecture can use self-management, self-healing, and self-security techniques to enhance the reliability, security, and safety of cloud computing. This makes it a more viable option for processing and cost-effectively storing large volumes of data. According to [4], there are specific areas that require improvement to make the cloud environment more secure. These include security awareness, training and education, and the shared responsibility model. These important concepts are explained below:

➢ *Security Awareness:*

This is often overlooked as a factor affecting cloud security architecture. Most of a security expert's time is spent on implementing controls, detecting intrusions, assessing risks, and managing security proactively or reactively. However, employees need to understand how their actions, even minor ones, can significantly impact the overall security of an organization. Both cloud clients and cloud providers must recognize the importance of securing information and protecting organizational assets [10]. Security awareness within an organization refers to how aware its personnel are of the importance of security and the controls in place. In addition to its benefits and objectives, an organization can gain the following advantages by implementing security awareness:

- It can reduce unauthorized actions by personnel.
- It can improve the effectiveness of existing security controls.
- It helps prevent fraud, waste, and abuse of computing resources.

Employees are considered "security aware" when they clearly understand the need for security, how security affects

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep164

business operations and the bottom line, and the daily risks to cloud computing resources. It is important to hold regular awareness meetings to train new employees and refresh the knowledge of existing ones. The material presented should be direct, simple, and clear. Several studies [11, 12, and 13] suggest the following activities to improve security within an organization without incurring high costs or consuming too many resources:

- An interactive presentation involving lectures and videos.
- Publishing content through posters, company newsletters, bulletins, and the intranet.
- Motivational efforts such as recognizing and appreciating achievements related to security.

➢ *Capacity Building Programs*

The study in [24] highlights that effective training programs are essential for equipping individuals with the knowledge and skills needed to protect cloud-based systems and data from cyber threats. Education provides a more formal way to protect data through classes, workshops, and even individual coaching. Here are the types of training associated with cloud security:

- Security-related job training for operators and specific users.
- Practical security training for IT operational personnel, system administrators, and system auditors.
- Security training for senior managers, functional managers, and business unit managers

Fig 3 Capacity Building Program Among Staff

Training and education for systems personnel, auditors, and security professionals are very important and often essential for business growth. It is also crucial to provide specific training on cloud security software and hardware to ensure the safety of the enterprise. Encouraging staff participation is a top priority in any training program, and they must understand how security impacts the organization's financial performance.

➢ *Shared Responsibility Model*

The author of [14] emphasizes that "it is vital for an organization to monitor, identify, and resolve any potential threats and misconfigurations on their cloud assets." This means that every organization should take this into account when managing information security in the context of cloud architecture. Microsoft® Azure™ [16] provides services that help users fulfill their security, privacy, and compliance requirements. This helps clarify the relationship between cloud service providers (CSPs) and their customers, outlining the roles and responsibilities of each party.

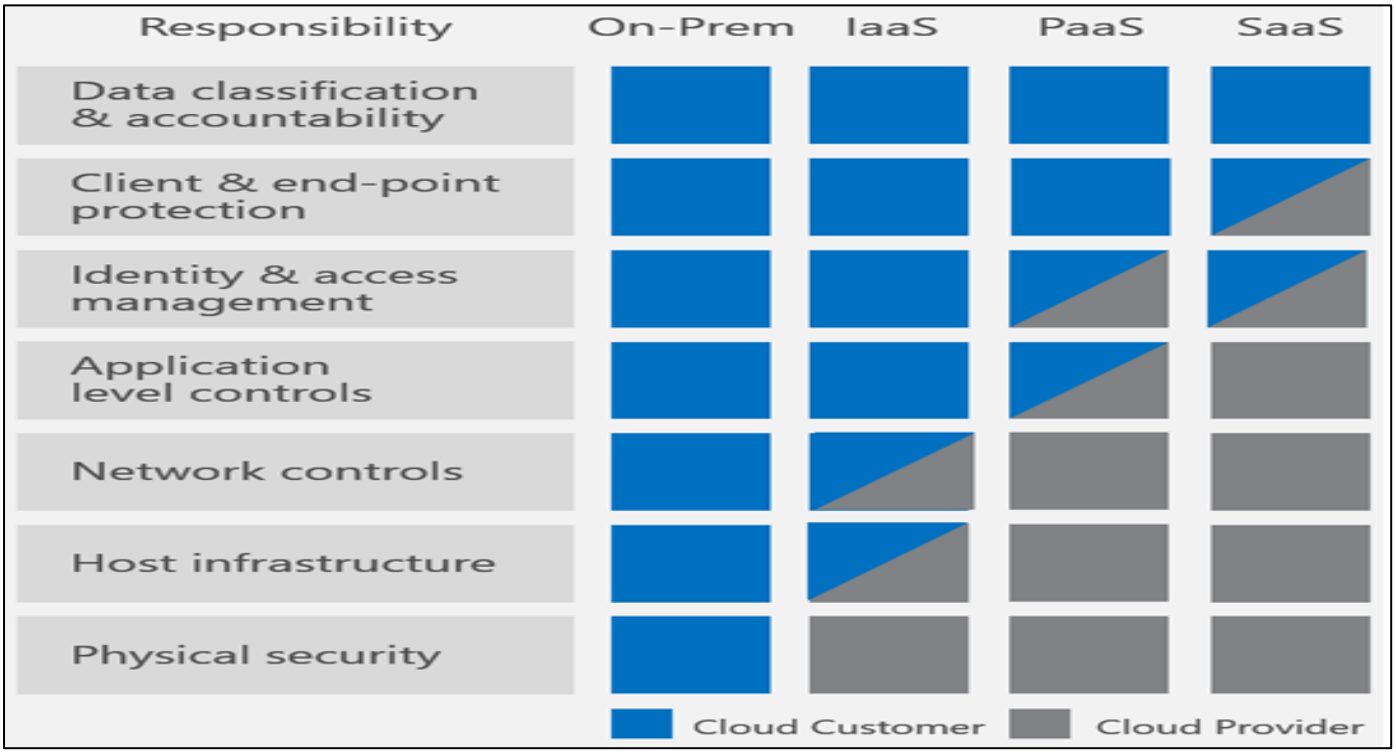

Fig 4 Seven Duties that Organizations should Consider

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep164

In Figure 4, the leftmost column shows seven duties that organizations should think about. These responsibilities help in creating a compliant and secure computing environment. The customer is responsible for making sure that data and its classification are done properly and that the solution meets all regulatory requirements. Physical security is a responsibility that entirely belongs to cloud service providers when using cloud technology. The rest of the responsibilities are shared between the customer and the cloud service provider, and both need to manage and handle them together. The Shared Responsibility Model can be explained as follows:

- *Data Classification and Accountability:*

The cloud user is responsible for ensuring that their solution and data are securely recognized, categorized, and properly classified to meet any required agreements. Cloud users must clearly distinguish between sensitive data and public data. SaaS solutions such as Office 365 and Dynamics 365 offer features to protect customer data, such as Office Lockbox and Data Loss Prevention. However, ultimately, the user is responsible for managing, classifying, and configuring the solutions to meet their specific security and agreement needs.

- *Client and Endpoint Protection:*

It are also important to clearly define user limitations and recognize responsibilities for the devices used to access cloud services. Cloud service providers may offer tools to manage end-point devices, such as Microsoft Intune, which provides secure device management and mobile application management capabilities. However, cloud users are still responsible for these issues.

- *Identity and Access Management:*

Identity control is a fundamental service that organizations provide continually, in ways that are easy to use and manage. Identity and access management allows users to access and use resources within their environment.

- *Application-Level Control:*

Platform-managed applications and services, such as web services, batch, docDb, IoT, media services, and others, simplify user responsibilities by offering a more secure solution managed by the CSP. While users need to configure the services correctly, these applications provide broader security capabilities and can integrate with other solutions, such as identity management.

- *Network Control:*

This includes the configuration, management, and securing of network elements like virtual networking, load balancing, DNS, and gateways. These controls enable services to communicate and work together effectively.

- *Host Infrastructure:*

The responsibility here involves configuring, controlling, and securing the computing infrastructure, such as virtual hosts, containers, service fabric, and auto scaling. It also includes storage options like object storage, CDN, file storage, and platform services. The CSP operates and secures the host services, including the operating systems of the service. In IaaS models, there is a shared responsibility between the CSP and the client to ensure the service is properly configured and secured. This includes setting up authorizations and network access controls to ensure that networks can communicate properly and that devices can correctly assign or support the right storage devices.

- *Physical Security:*

Customers often see the most obvious benefit of moving services to the cloud as the management of the physical environment. CSPs have security processes and strategies to protect the infrastructure from unauthorized physical access. According to Microsoft, other physical security considerations include features such as cooling, air quality management, device management, and power regulation.

VI. CONCLUSION

Information security is a major topic today, and more users are turning to cloud computing primarily due to security concerns related to data. However, cloud storage security is not just an official issue; it also involves adjustments, management, and compliance with laws and regulations. This paper provides an overview of information security challenges in cloud computing. It briefly describes data integrity, confidentiality, and availability related to cloud services, and outlines common cloud attacks. It also reviews the Shared Responsibility Model, which outlines seven responsibilities performed by cloud suppliers to help consumers meet their security, privacy, and agreement needs.

REFERENCES

[1]. Rizwana A.R. Shaikh ; Masooda M. Modak "*Measuring Data Security for a Cloud Computing Service"* 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pages: 1 – 5.

[2]. Preeti Sirohi ; Amit Agarwal *"Cloud computing data storage security framework relating to data integrity, privacy and trust"* 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Pages: 115 – 118.

[3]. Fuguo Li, "Study on security and prevention strategies of computer network" 2012 International Conference on Computer Science and Information Processing (CSIP).

[4]. Ronald L, Krutz and Rusell Dean Vines "A Comprehensive Guide to Secure Cloud Computing" Wiley Publishing.Inc, 2010. Page 177-190.

[5]. What's Special about Cloud Security? Peter Mell IT Professional Year: 2012 Volume: 14, Pages: 6 – 8

[6]. Deepak R Bharadwaj ; Anamika Bhattacharya ; Manivannan Chakkaravarthy '*Cloud Threat Defense – A Threat Protection and Security Compliance Solution*" 2018 IEEE

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep164

International Conference on Cloud Computing in Emerging Markets (CCEM)

[7]. *"A Semantic Approach to Cloud Security and Compliance* "Amit Hendre ; Karuna Pande Joshi 2015 IEEE 8th International Conference on Cloud Computing Year: 2015 Pages: 1081 – 1084.

[8]. Randeep Kaur ; Jagroop Kaur "*Cloud computing security issues and its solution: A review "* 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) Pages: 1198 – 1200.

[9]. Xiaoling Sun "*The study on computer network security and precaution"* Proceedings of 2011 International Conference on Computer Science and Network Technology. Volume: 3 Pages: 1695 – 1698

[10]. Asım Gençer Gökce "*The public information systems security program"* International Conference on Information Society (Society 2012), Pages: 352

[11]. "*Teaching for Conceptual Change in Security Aware ness"* Yuen-Yan Chan ; Victor K. Wei IEEE Security & Privacy, 2008 Volume: 6 , Issue: 6, Pages: 67 – 69

[12]. "*Security Oriented Malicious Activity Diagrams to Support Information Systems Security"* Othmar O. Mwambe ; Isao Echizen 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Pages: 74 – 81

[13]. *"Study on Data Security Policy Based on Cloud Storage* "Diao Zhe ; Wang Qinghong ; Su Naizheng ; Zhang Yuhan 2017, Pages: 145 – 149

[14]. "*Data Access Security in Cloud Computing: A Review* " Anagha Markandey ; Prajakta Dhamdhere ; Yogesh Gajmal 2018 International Conference on Computing, Power and Communication Technologies (GUCON). Pages: 633 – 636

[15]. "*Security risks and their management in cloud computing"* Afnan Ullah Khan ; Manuel Oriol ; Mariam Kiran ; Ming Jiang ; Karim Djemame 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, 2012, Pages: 121 – 128.

[16]. Microsoft *"Shared Responsibility for Cloud Computing"* April 2017, Version two.

[17]. Udupa A, T., Jayaram, S., & Hegde, S. G. (2024). A Brief Study of Computer Network Security Technologies. *arXiv e-prints*, arXiv-2403.

[18]. Bibartiu, O., Dürr, F., Rothermel, K., Ottenwälder, B., & Grau, A. (2024). Availability analysis of redundant and replicated cloud services with Bayesian networks. *Quality and Reliability Engineering International*, *40*(1), 561-584.

[19]. Krishna, G. J. (2024). Serial Parallel Reliability Redundancy Allocation Optimization for Energy Efficient and Fault Tolerant Cloud Computing. *arXiv preprint arXiv:2404.03665*.

[20]. Sharma, T., Wang, T., Di Giulio, C., & Bashir, M. (2020). Towards inclusive privacy protections in the cloud. In *Applied Cryptography and Network Security Workshops: ACNS 2020 Satellite Workshops, AIBlock, AIHWS, AIoTS, Cloud S&P, SCI, SecMT, and SiMLA, Rome, Italy, October 19–22, 2020, Proceedings 18* (pp. 337-359). Springer International Publishing.

[21]. Bomström, T. (2024). *Case study: cloud computing model for vehicular data processing* (Master's thesis, T. Bomström).

[22]. Kumar, A., Rani, S., Rathee, S., & Bhatia, S. (Eds.). (2023). *Security and risk analysis for intelligent cloud computing: methods, applications, and preventions*. CRC Press.

[23]. Taneja, A. K., Kumawat, P., & Asthana, B. SECURITY ISSUES ON CLOUD COMPUTING.

[24]. Khan, W. (2023). *Developing and delivering comprehensive cloud security training programs: The importance of continuous education in maintaining high levels of security awareness. International Journal of Advanced Research in Engineering and Technology*, *14*(7), 132–156.