ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1045

Cybersecurity Risks in Cloud Computing and Data Breaches: Implications and Mitigation Strategies for Nigerian Organizations

Abraham Omatule Victor[1]; Musa Martha Ozohu[2]

[1,2] Centre for Peace and Security Studies,
University of Port Harcourt,
Port Harcourt, Nigeria

Publication Date: 2026/01/30

Abstract: In order to make significant changes to their digital life, a large number of enterprises all around the world, including those in Nigeria, are adopting cloud computing. In this paper, we investigate what other people have written and what is happening in Nigeria in order to determine the most significant cybersecurity risks that are associated with cloud environments, the factors that lead to cloud-related data breaches, the consequences of such breaches, and the strategies that can be implemented to mitigate these risks while adhering to Nigeria's regulations and infrastructure. According to the findings of the survey, the most common causes of security breaches are still human mistake, inadequate management of identity and access, and inadequate management of configuration. In it, it is stated that the implementation of Zero Trust security models, constant monitoring of the situation, training of employees, and strict adherence to national and international data protection regulations are all components that can contribute to the improvement of cloud security resilience.

Keywords: *Component; Cloud Computing, Cybersecurity, Data Breaches, Risk Management, Zero Trust, Identity And Access Management.*

How to Cite: Abraham Omatule Victor; Musa Martha Ozohu (2026) Cybersecurity Risks in Cloud Computing and Data Breaches: Implications and Mitigation Strategies for Nigerian Organizations. *International Journal of Innovative Science and Research Technology*, 11(1), 2293-2298. https://doi.org/10.38124/ijisrt/26jan1045

I. INTRODUCTION

It is now well acknowledged that cloud computing is an essential component of the digital infrastructure that we utilize on a daily basis. Because it provides companies with access to computing resources whenever they require them, it eliminates the need for those organizations to worry about maintaining a record of actual hardware. According to the National Institute of Standards and Technology (Mell & Grance, 2011), cloud computing makes it simple to gain access to shared pools of configurable resources. These resources include networks, storage, applications, and services that can be set up quickly and with no effort on the part of administrators. A great number of domains have witnessed accelerated innovation and increased efficiency as a result of this approach. Companies of significant size, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, are actively advocating for its implementation in every region of the world. In spite of the fact that these are positive aspects, moving away from traditional on-premise systems and toward cloud-based solutions is detrimental to secure information. In contrast to traditional information technology systems, which are exclusively functional in certain regions, cloud infrastructures are able to function in environments where a large number of individuals share and connect to the same items. As a result, it becomes more difficult to maintain security and makes it simpler for cybercriminals to gain access. A significant number of cloud data breaches are the result of weaknesses that might have been avoided. These flaws include inadequate configuration procedures, insecure application interfaces, weak access controls, and poor security governance. The utilization of cloud computing is continuing on the rise in Nigeria, particularly in sectors such as the government, education, telecommunications, and finance. However, preparation in terms of cybersecurity has not always been able to keep up with this rapid increase. Persistent vulnerabilities have been caused by a number of factors, including gaps in regulatory compliance, a shortage of experienced cybersecurity workers, a lack of investment in security technologies, and a lack of understanding of shared responsibility models. Because of these factors, it is very necessary to give serious consideration to the risks associated with cloud cybersecurity in Nigeria's own institutions and infrastructure.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1045

II. CLOUD COMPUTING RISKS TO CYBERSECURITY

➢ *Misconfigurations*

Settings that are incorrect or faults in system configuration are one of the most prevalent and easy-to-avoid reasons why cloud systems fail to provide adequate security. It is expected that cloud computing systems would provide users with a great deal of flexibility and power; nevertheless, this freedom may become problematic if the security settings are not properly understood or utilized. In the event that you make a little mistake, such as leaving a storage service open to the general public or incorrectly configuring the rules of a firewall, you could be able to expose confidential company information on the internet without the company being aware of it. When it comes to traditional information technology environments, configuration tasks are typically handled by security specialists who are employed continuously. Nevertheless, in the cloud, developers, system administrators, and operational workers are performing an increasing number of these activities, despite the fact that they may not always have a great deal of knowledge regarding security. Because of this alteration, the likelihood of errors occurring is increased, particularly in settings where speed is more important than conducting rigorous security checks. Common concerns with the configuration of a system include granting excessive access to storage containers, granting an excessive number of rights to networks, and failing to restrict the capabilities of administrators. Even though these vulnerabilities would not be immediately apparent during normal operations, they could be discovered by attackers in a short amount of time using automated scanning techniques. Those businesses who make use of more than one cloud platform have an even more difficult challenge. Due to the fact that every provider has their own interfaces and default security settings, it is difficult to stay up with the same security requirements. As a result of the fact that they might remain open for an extended amount of time in the absence of solid governance structures, regular audits, and persistent monitoring, misconfigurations are one of the most prevalent security flaws available in current cloud computing systems.

➢ *Weak Identity and Access Management (IAM)*

A poor management of IAM, which stands for Identity and Access Management, is the most important aspect of cloud computing security since it determines who is allowed to use digital resources. In situations where identity and access management (IAM) methods are not well thought out or implemented, attackers have the ability to simply enter services that they should not be able to and move freely between them. This puts the confidentiality, integrity, and availability of the company's data in a very precarious position. A significant number of cloud security problems are brought on by the theft of login information. Attackers frequently obtain these credentials by deceiving users through the use of social engineering techniques, phishing emails, or fake login pages. These methods are designed to exploit people's trust in one another. As a result of the fact that many individuals use the same password on multiple websites, the problem has become even more severe. Once hackers have gained access to a single account, they are often able to utilize the same information to obtain access to a considerable number of other systems, including cloud-based applications and storage services. Despite the implementation of these approaches, businesses who do not have robust authentication systems are still susceptible to automated attacks such as brute-force attacks and password spraying attempts. Due to the fact that users have an excessive amount of privileges, it is likely that attackers will be able to acquire further rights and access important sections of the system after they have successfully achieved initial access. It is possible for enterprises to leave their cloud environments vulnerable to attack if they do not implement multi-factor authentication, stringent password restrictions, and regular access checks. The identity of the user is the primary security barrier in the cloud-based world of today, which has entirely replaced physical networks. This indicates that even the most robust technical safeguards are susceptible to being compromised by inadequate IAM practices.

➢ *Insecure Application Programming Interface*

Application Programming Interfaces (APIs) that are not secure APIs, which are also known as application programming interfaces, are the components of contemporary cloud computing systems that are not visible to the naked eye. They make it simple for applications to communicate with one another, carry out tasks in an automated fashion, and provide digital services. APIs, despite the fact that they are quite important, are generally not included in security strategies. Because of this, hackers will find them to be easy targets. If application programming interfaces (APIs) do not have robust authentication procedures, adequate encryption, or restrictions on how they can be used, they have the potential to put sensitive data and essential system functions at risk. It is possible for individuals that are interested in stealing data, modifying transactions, or entering backend services without authorization to take advantage of these vulnerabilities. APIs, in contrast to more conventional user interfaces, frequently operate beneath the surface. Because of this, it is possible that security teams will not always be able to determine how individuals are utilizing or abusing them. Attackers are more likely to target application programming interfaces (APIs), which might often have less robust security, while organizations work to make their websites and front-end applications more secure. If these interfaces do not have sufficient API governance, such as frequent security testing, tight access limits, and persistent monitoring, they have the potential to become quiet doors for huge breaches. In cloud contexts, where automation and integration are essential to the functioning of things, securing application programming interfaces (APIs) is not merely an additional step; rather, it is an essential component of cybersecurity.

➢ *Multi-Tenancy Risks*

The presence of more than one tenant is one of the most significant aspects of public cloud computing, and one of the risks associated with multi-tenancy is the possibility of having more than one tenant. Under this model, a large number of customers use the same physical infrastructure, but they continue to believe that they are distinct individuals. Cloud service providers spend a significant amount of money on technologies that facilitate the separation of components; nevertheless, due to the fact that this environment is shared, it is less secure than traditional private systems. The presence of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1045

a defect in a shared component, such as the hypervisor or a common service, could provide an opportunity for attackers to move between different tenant configurations. The occurrence of these kinds of things can allow an individual to gain access to data that is not theirs, prevent shared services from operating, or exacerbate existing supply chain security issues. A security breach that initially affects only one customer has the potential to become a problem for the entire platform in the most exceptional of circumstances. The fact that these dangers frequently occur deep within the infrastructure of the provider, where particular customers are unable to take any action to save themselves, makes them particularly terrifying. For this reason, businesses need to have a great deal of faith in the security measures, certifications, and compliance standards that their cloud providers have in place. It is necessary for them to simultaneously establish robust internal safeguards such as encryption, monitoring, and access controls in order to substantially reduce the danger that they face. Security is something that both customers and suppliers need to be committed to in order to deal with the risks that come with multi-tenancy.

- *Insider Threats*

When it comes to cloud security, insider attacks are one of the most difficult challenges to address because they originate from individuals who already have authorization to use the organisation's systems. It is possible that these individuals are employees, independent contractors, or business partners who have been presented with private assignments to carry out. Deliberate insider risks include stealing data or disrupting a system, whereas inadvertent insider risks include being careless, not knowing about it, or falling for phishing attacks. Both types of insider risks are possible. What insiders do is frequently more detrimental than what outside foes do since they are familiar with the inner workings of the organization. A person with more influence within the organization has the ability to breach the rules, reveal sensitive information, or discontinue essential services. The occurrence of this kind of behavior is exceedingly difficult to observe in cloud-based systems, because access is often granted remotely and is contingent on particular duties. Companies that do not have stringent access limits, substantial audit records, or a habit of keeping an eye out for anomalous user behavior are more likely to be victims of insider threats. In the event that these preventative measures are not followed, devastating events may take place without anyone being aware of them until a significant amount of harm has already been done. To protect against the dangers posed by insiders, you need more than just technical safeguards. In addition to this, you need to have strong business regulations, programs that teach employees about those policies, and a culture that emphasizes accountability.

- *Limited Visibility in Multi-Cloud Environments*

The inability to see clearly in locations that contain more than one cloud Many companies use multi-cloud solutions in order to be more flexible, to avoid being dependent on just one vendor, and to keep their operations running. In spite of the fact that this method of doing things appears to have some practical advantages, it also makes it significantly more challenging to monitor security operations. It is difficult to maintain track of risk in a consistent and unified manner due to the fact that every cloud provider has a different set of management tools, monitoring systems, and security frameworks. This lack of centralized visibility frequently results in security processes that are not of very high quality. It is possible that policies may not be enforced in the same manner across all platforms, that risks will go unreported for an extended period of time, and that reaction efforts to incidents would become disconnected. It is not always simple for security teams to keep track of where sensitive data is stored, who has access to it, and whether or not policies are being executed in a consistent manner across all settings. When confronted with scenarios of this complexity, attackers commonly focus their attention on the weakest point of the system, which is typically the cloud platform that is not being monitored carefully or that is not being configured appropriately. Not only does limited visibility make it more difficult to spot breaches, but it also gives attackers more time to move between systems and make their damage even more severe. Companies that operate in multi-cloud environments need to have centralized governance, integrated monitoring, and coordinated incident response in order to maintain a high level of cybersecurity.

III. CAUSES AND EFFECTS OF CLOUD DATA BREACHES

- *Causes*

Why The most usual causes of cloud data breaches are storage systems that aren't set up correctly, IAM roles that are too open, and firewall rules that aren't clear. Providing users with an excessive amount of access allows them to roam throughout networks without permission, which can occasionally put private information at risk. Storage systems that are available to the public can sometimes put private information at risk. Insufficient or stolen credentials are the root cause of a great deal of cloud-related problems. The methods of phishing, social engineering, and credential stuffing are utilized by attackers in order to gain access to systems. When information is being provided or stored, it must be protected from unauthorized access. In the event that it is not, breaches have a greater impact because that is when attackers are able to quickly employ the data. There are still a lot of companies who are slow to implement zero trust security approaches. Rather than that, they make use of obsolete models that are built on perimeters and do not check things on a consistent basis. Insecure application programming interfaces (APIs) and slow software updates make things more vulnerable. Additionally, insufficient logging and monitoring frequently make it difficult to uncover inappropriate activity in a timely manner.

- *Effects*

In the event that data stored in the cloud is stolen, the consequences extend beyond the immediate loss of financial resources. Investigations, repairs, legal expenditures, fines from authorities, and harm to a company's reputation that lasts for a long time are all expenses that businesses are required to pay financially. It happens rather frequently that operations have to be halted because systems need to be pulled offline in order to perform forensic analysis and recovery. These issues get even more difficult when customers quit trusting you,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1045

which causes them to leave and thus makes the market less certain.

IV. THEORETICAL FRAMEWORK

There are three key theoretical points of view that work together in this study to help us realize the risks associated with cybersecurity in cloud computing systems. These theoretical frameworks allow us to better understand the risks. One of these perspectives is the CIA triad, another is the zero trust architecture, and yet another is the risk management philosophy. In each framework, security is approached from a different perspective, with the goal of determining what needs to be protected, how protection should be enforced, and how risks should be managed in an intelligent manner.

➢ *The Three Components of the Central Intelligence Agency*

The CIA Triad is one of the most well-known and enduring models to emerge from the subject of information security. It is an acronym that stands for Availability, Integrity, and Confidentiality. In it, the three qualities that must be present in any knowledge system in order for it to be considered secure are discussed. The concept of confidentiality refers to the protection of information from individuals who are not authorized to view or discuss it. It may be challenging to maintain the confidentiality of data in cloud computing systems due to the fact that the data is stored in remote locations and can be accessed via the internet. Inadequate access limits, phishing efforts, stolen login credentials, and abuse by employees within the organization are all examples of threats that increase the likelihood that confidential information could be made public. When firms fail to protect their customers' privacy, they run the risk of getting into a lot of difficulty, including being penalized, losing the trust of stakeholders, and having their reputations damaged. When we talk about integrity, we mean that the information is correct and trustworthy. It guarantees that the information will remain unchanged, complete, and accurate unless it is altered by a person who has been granted authorization to do so. Cloud computing systems are susceptible to data integrity issues due to a variety of factors, including malicious software assaults, unauthorized changes to configuration settings, software defects, and human input errors. In situations where there is a breach of integrity, organizations may make judgments based on information that is deceptive. There is a possibility that this will have an impact on the rule-following, operational efficiency, and financial reporting. The term "availability" refers to the fact that the systems, services, and data are always present whenever they are required. When it comes to cloud settings, availability is of utmost importance because the majority of business activities are dependent on the capacity to access digital platforms without encountering any difficulties. Threats such as distributed denial-of-service attacks, ransomware, infrastructure failures, and prolonged service outages have the potential to prevent businesses from operating, cause them to lose money, and damage their reputations. When we take into consideration all of the key cyber risks at the same time, the CIA Triad assists us in understanding how each of these threats impacts the primary goals of information security. In this work, a paradigm is utilized to demonstrate how common cloud-related risks, such as misconfigurations, inadequate identity controls, and insider assaults, pose a direct threat to the fundamental principles of confidentiality, integrity, and availability.

➢ *The Structure of Zero Trust*

Businesses now have the ability to employ Zero Trust Architecture to think about cybersecurity in a different way. According to conventional security models, personnel and devices that are located within the network of an organization can normally be trusted, whereas those that are located outside of the network are considered to be potential threats. On the other hand, this is no longer the case in the modern digital world, where cloud services, remote work, and interfaces provided by third parties have made it more difficult to differentiate between one corporation and another. Zero Trust is based on a fundamental principle that is both elementary and profound: you should never put your faith in anyone. Instead, it is necessary to check each and every request to access a resource or system, regardless of the region from which it originated. This model performs constant checks and approvals on individuals, devices, and programs before allowing them to enter the computer system. For a number of reasons, this method functions most effectively with cloud-based applications. Given that users can access cloud systems from a wide variety of locations, including their own devices and networks that are not connected to the cloud, it is difficult to establish a typical security barrier surrounding cloud computing. There are new risks that are being introduced as a result of the growing prevalence of the use of external service providers by businesses. When it comes to network security, identity is frequently the first line of defense, rather than the physical boundaries of the network. The concept of limited access rights, which means that users only receive the permissions they require to carry out their responsibilities, is one of the fundamental notions that underpins zero trust. Ongoing verification entails assessing trustworthiness each and every time you engage in conversation with a person, and not only when you log in. Once an attacker has gained access to an account, it is more difficult for them to travel throughout the system because of the segmentation of systems. Continuous monitoring that assists you in locating activity that is problematic in a timely manner. By adhering to these standards with Zero Trust, the likelihood of someone within the company stealing credentials or using them in an inappropriate manner is reduced. They are unable to easily move between systems, even if they are successful in breaking in. A realistic approach to addressing contemporary cloud security challenges, such as inadequate identity management, insider threats, and undesired lateral movement, is shown in this paper through the utilization of Zero Trust Architecture.

➢ *The Theory of Risk Management*

The theory of risk management provides us with a method to think about cybersecurity in a strategic manner by recognizing the fact that no system can be totally safe. It should not be the goal of organizations to defend everything notwithstanding the expenses involved. When it comes to risk management, they should instead take a methodical and well-informed approach. Before making judgments on security, it is recommended, according to this idea, that you give serious consideration to potential threats and the consequences that may emerge from them. It is suggested by ISO 31000 and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1045

other international standards that risk management is an ongoing activity that consists of three essential steps: being aware of potential dangers, such as faults and threats, as well as the potential ways in which an attack could occur. when determining how to deal with a threat, it is important to take into consideration both the frequency with which it may occur and the severity of the consequences that it may have. Dealing with risks by taking measures such as preventing them, reducing them, transferring them, or accepting them or accepting them as they are. When it comes to matters of cybersecurity, this approach assists firms in making informed decisions regarding how to best use of the limited resources they have available. It is possible for those who make decisions to concentrate on ensuring the safety of the most important data and systems rather than making an effort to safeguard everything in the same manner. In addition, the theory of risk management outlines a range of security safeguards that businesses may implement. For instance, firewalls, access controls, and encryption are all examples of preventive measures that halt attacks before they occur. Real-time threat detection is made possible by detection technologies such as intrusion detection systems and monitoring tools. Examples of these technologies include. Recovery strategies include, for instance, backup systems and plans for responding to disasters. These are examples of recovery tactics that help things return to normal as fast as possible following a breach. Some of the ways that inappropriate behavior can be stopped include the implementation of policies, disciplinary procedures, and staff awareness initiatives. Because of this principle, businesses who operate in regions where money and technology are difficult to come by can benefit greatly from its application. A strategy that is well-balanced and ensures that security actions are in accordance with the organization's goals and the law is encouraged by this aspect. Through the use of risk management theory, this study demonstrates how Nigerian organizations may implement a plan that is both practical and cost-effective in order to address cloud security concerns. By combining their respective strengths, the CIA Triad, Zero Trust Architecture, and Risk Management Theory all contribute to the development of a solid theoretical foundation for this study. The information that we need to preserve is the availability, the confidentiality, and the integrity of the information, as stated by the CIA Triad. The Zero Trust Architecture provides an explanation of how to maintain security in contemporary cloud computing systems that are decentralized. Through the application of the idea of risk management, one can learn how to prioritize risks and deal with them in a manner that is logical. By combining these three points of view, the study creates a comprehensive framework for analyzing cloud computing cybersecurity challenges and developing solutions that are both practical and helpful, and that are tailored to meet the operational and regulatory requirements of Nigerian enterprises.

V. A DISCUSSION OF EMPIRICAL EVIDENCE

Misconfigurations, inadequate identity and access management (IAM) restrictions, and inadequate governance are widely cited as important contributors to cloud security problems in empirical studies. Misconfigurations are the root cause of a significant number of security breaches, and the exploitation of stolen credentials continues to be one of the most common methods of attack utilized. Many businesses in Nigeria are still not very knowledgeable about cloud security controls and the legal requirements that they must fulfill in order to ensure the safety of their data.

VI. EVOLUTION OF LITERATURES ON CLOUD SECURITY

The initial research focused mostly on determining what cloud computing is and the dangers that are associated with the utilization of virtual machines. This led to the development of the literature on cloud security. In subsequent research, the shortcomings of service delivery models such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) were investigated. In the field of cybersecurity, recent research has demonstrated how challenging it is to make use of numerous clouds, secure containers, implement Zero Trust principles, and engage in artificial intelligence techniques.

VII. RESEARCH GAPS

There are not many studies that focus solely on cloud environments in Africa and Nigeria. This is a gap in the research situation. Putting together threats, breaches, and remedies to stop them all at the same time is not something that many models do. Additionally, there has not been a significant amount of research conducted on regulatory frameworks such as the Nigeria Data Protection Regulation for academic writing.

VIII. MITIGATION STRATEGIES

- *Technical Measures*

The use of encryption for data when it is not being used and when it is being delivered, the use of multi-factor authentication, and the partitioning of networks into smaller pieces in order to reduce the amount of lateral movement within systems are all examples of good technical controls.

- *Administrative Measures*

Businesses should make it a priority to educate their staff members about the importance of safeguarding their information resources. In addition to this, they should conduct regularly scheduled audits and risk assessments, and they should make certain that both cloud providers and clients adhere to the shared responsibility model.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1045

- *Regulatory Measures*

It is of the utmost importance to adhere to the Nigeria Data Protection Regulation as well as the standards established by the NITDA. The utilization of international standards such as ISO 27001 and NIST 800-207 results in an improvement in the quality of security governance.

- *Governance of Vendor Relationships*

It is important to regularly check service-level agreements, vendor security certifications, and the cloud posture.

IX. CONCLUSION

Cloud computing presents Nigerian organizations with a multitude of new opportunities; yet, it also makes it more difficult for them to maintain the security of their data. A significant number of breaches that are associated with cloud computing are not triggered by complex attacks but rather by security flaws that could have been avoided. When it comes to cloud security, we need to take a comprehensive approach that includes not just technical measures but also good governance, adherence to the regulations, and training for the employees. Businesses have the potential to significantly reduce their susceptibility to cyberattacks by putting into practice the Zero Trust principles, strengthening their monitoring capabilities, and ensuring that their security strategies adhere to the laws and norms of Nigeria.

REFERENCES

[1]. Alharkan, I., & Aslam, N. (2021). *Risk factors and mitigation approaches in cloud computing: A comprehensive review*. Journal of Cloud Computing, 10(3), 1–18.
[2]. Almorsy, M., Grundy, J., & Müller, I. (2016). *An analysis of the cloud computing security problem*. Journal of Cloud Security, 4(1), 1–18.
[3]. Adeniran, A., Oluwole, S., & Adeyemi, T. (2023). *Cloud adoption practices and cybersecurity readiness in Nigerian organizations*. African Journal of Information Systems, 15(2), 55–72.
[4]. CISA. (2022). *Analysis report: Capital One cloud misconfiguration breach*. Cybersecurity and Infrastructure Security Agency.
[5]. ENISA. (2023). *ENISA threat landscape for cloud computing 2023*. European Union Agency for Cybersecurity.
[6]. Hashizume, K., Rosado, D., Fernández-Medina, E., & Fernández, E. (2022). *An updated classification of security threats in cloud computing*. Computers & Security, 113, 102–119.
[7]. IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Security.
[8]. Ibrahim, U., & Salawu, R. (2022). *Cloud security awareness and NDPR compliance among Nigerian enterprises*. Nigerian Journal of Information Security, 8(1), 22–36.
[9]. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing (SP 800-145)*. National Institute of Standards and Technology.
[10]. NITDA. (2021). *Nigeria cloud computing policy guidelines*. National Information Technology Development Agency
[11]. Subashini, S., & Kavitha, V. (2011). *A survey on security issues in cloud computing*. Journal of Network and Computer Applications, 34(1), 1–11.
[12]. Takahashi, Y., Sato, K., & Nakamura, T. (2023). *Emerging security challenges in multi-cloud environments*. Journal of Cybersecurity Research, 7(4), 45–62.
[13]. Verizon. (2024). Data Breach Investigations Report 2024. Verizon Enterprise