International Journal of Computer Science and Engineering Innovations
ISSN: 3107-9458 | Volume 1 Issue 2, 15-22, October-December 2025
DOI: https://doi.org/10.64137/31079458/IJCSEI-V1I2P103

Scholastic Research Publication

Received: 27/11/2025 Revised: 30/11/2025 Accepted: 09/12/2025 Published: 13/12/2025

Original Article

Cloud-Based Storage Systems and Data Security in Organisations: An Explorative Review

TIMINEBIERI PETER EKE
Department of Computer Science, Niger Delta University, Bayelsa State, Nigeria.

ABSTRACT: *The increasing dependence on digital data has made effective data storage and protection an essential issue in organisations around the world. Data loss, cyber threats, poor infrastructure, and high costs of service maintenance of the traditional on-premises storage are the persistent issues that many organisations in Nigeria are grappling with. Due to this, cloud-based storage systems have been introduced as an option to enhance data management and security. This paper will consider the cloud-based storage systems and effective data protection within the context of Nigerian organisations, with particular regard to the impact of cloud-based storage on data protection and the issue of data security within the cloud environment, and how it can be effectively maintained. The approach used in the study is literature-based, relying on the available scholarly materials, policy documents, and empirical studies on cloud computing, data protection, and organisational information systems. Results of the reviewed literature show that various cloud-based storage systems have the potential to address the protection of the data, in terms of data availability, confidentiality, integrity, and disaster recovery, due to the availability of the following features: encryption, automatic backups, access control measures, and monitoring of the system at all times. Such advantages are of special importance to the Nigerian context, where organisations are usually limited by the unstable power supply and a lack of ICT infrastructure. Nevertheless, the research also indicates that Nigerian organisations have a number of difficulties associated with the provision of efficient data protection with the help of cloud-based storage systems. Such difficulties are the lack of technical skills, the insufficient knowledge of the cloud security roles, the lack of a data governance system, the problems of regulatory compliance, and the problems of infrastructure. The research concludes that although cloud-based storage systems have a huge potential of enhancing data security in the organisations of Nigeria, their application is influenced, to a great extent, by the organisational capacity, adherence to regulatory requirements, and commitment of the management to ensure safety in using cloud computing. The research suggests improved data protection policies, employee education, regulatory assistance, and strategic cloud adoption to improve the results of data security.*

KEYWORDS: *Cloud computing, Cloud-based storage systems, Data protection, Information security.*

1. INTRODUCTION

The fast-growing Information and Communication Technology (ICT) has dramatically changed the way organisations generate, store, handle, and safeguard data. Cloud computing, and more specifically, cloud-based data storage systems, can be regarded as one of the most evident technological advances that define the current data management trends. Cloud-based storage solutions enable organisations to keep data in remote servers under the control of third-party service providers and accessed via the internet instead of using only the conventional on-site storage infrastructure. The technological change has reconfigured the way data is managed in organisations as it brings about the benefits of scalability, flexibility, cost effectiveness, and enhanced accessibility (Marvis & Emmanuel, 2014).

Organisations worldwide are turning towards cloud storage systems in a bid to digitally transform their organisations. The increasing amount of data generated every day by organisations, and the necessity to have access to it in real time, as well as collaboration and efficient data processing, have rendered outdated the traditional storage systems outdated. Cloud storage systems offer a potential solution since they allow organisations to scale the storage capacity on command, save on hardware and maintenance expenditure, and enhance operational efficiency. Consequently, cloud computing is now a vital facilitator of business processes in the contemporary world and the provision of services to people by the government.

The applicability of cloud-based storage systems has continued to increase in Nigeria, where organisations have identified new ways of solving chronic problems related to data management. Limited resources in terms of finances, poor ICT infrastructure, and lack of technical know-how are some of the constraints affecting many organisations in Nigeria, particularly the public institutions and the small and medium-sized enterprises (SMEs). Cloud storage systems are a promising solution as they minimize physical server, data centre, and specialised IT staff requirements before heavy capital investment is required (Owoseni et al., 2025). Cloud computing is therefore becoming an important strategic instrument of promoting organisational efficiency and competitiveness in Nigeria.

Although the advantages are seen, the pace of adoption of cloud-based storage systems within Nigerian organisations is rather low and uneven. Although the adoption of cloud solution has been realised among big companies and multinational companies, a good number of native organisations are hesitant. Poor and unstable internet connectivity, fluctuating power supply, expensive bandwidth, and the issue of data sovereignty still act as some of the challenges that hinder widespread use. These structural constraints lower the security of cloud services and cast doubt on their appropriateness to mission-critical organisational information.

One issue that affects the adoption of cloud in Nigerian organisations is the issue of data protection. The term data protection (policies, technologies, practices) is employed to protect data against unauthorised access, loss, misuse, or breaches. Protecting the data within the cloud environments is even more complicated since the information is stored and processed beyond the immediate reach of the organisation. This casts doubts on the confidentiality, integrity, and availability of organisational data, including sensitive data of organisational data like financial records, employee data, and customer information (Garga & Sadiq, 2025).

The growing rate of cyber threats and data breaches in the world has increased the organisational sensitivity to the risk of data protection with cloud-based storage systems. Nigerian organisations are particularly susceptible, as they have poor cybersecurity systems, few data protection policies in force, and insufficient technical capacities. Cases of data leakage, hacking, and unauthorised access have raised questions about the security of clouds, and many organisations are either tempted to delay or adopt the cloud in a cautious manner (Businessday, 2025).

The regulatory environment is also influential in data protection practices in Nigerian organisations. The launch of the Nigeria Data Protection Regulation (NDPR) can be seen as a significant move to enhance the level of data privacy and protection in Nigeria. The regulation requires organisations to make sure that the processing of personal data is lawful, provide adequate security measures, and hold themselves accountable when using the services of third parties, including cloud service providers. Nonetheless, the issue of compliance with NDPR is still a challenge to most organisations because of the insufficient awareness, enforcement strategies, and challenges of aligning cloud services with the local requirements of the regulations.
Moreover, the information stored in cloud settings is prone to cross-border data transfers, and this raises more legal and ethical issues. The Nigerian organisations can save their data in servers that are not based in the country and subject them to international jurisdictions and regulatory frameworks. This makes it hard to govern and hold data accountable, especially in cases where data breaches have been realized. Consequently, organisations are faced with the challenge of weighing the advantages of cloud-based storage and the necessity to abide by national data protection legislation and have sufficient control over their data resources.

Human factors and organisational capacity also determine the effectiveness of data protection in the cloud-based storage systems. Nigerian organisations do not have a large pool of skilled individuals who have knowledge in cloud computing, cybersecurity, and data governance. The presence of this skills gap would enhance the chances of a poorly configured system, lax access controls, and ineffective monitoring that may endanger data security. The fact that employees have little knowledge of best practices in cloud security also presents organisations with insider attacks and unintentional data breaches (Disciplines.ng, 2024).

Also, organisational culture and perception of management have a great influence on cloud adoption and data protection practices. Research has indicated that the perceptions of the decision-makers towards the security risks of the cloud have a significant impact on their intentions to adopt the cloud-based solutions. In cases where the management is not convinced that cloud systems are secure and reliable, organisations are less prone to investing or embracing cloud technologies in their operations completely (Bakare, 2020). Such a reality has led to a more conservative approach where organisations apply cloud service in non-sensitive applications and keep sensitive data in local servers. Nigeria also has a cloud adoption decision based on economic reasons. Though it is usually advertised that cloud-based storage systems are cost-effective solutions, the initial expenses incurred during the migration, integration of the system, employee training, and the subscription fees can be high. Such costs may discourage cloud adoption by SMEs and the public sector organisations that have a strict budget constraint, even though in the long term they will be able to save on maintenance and increase efficiency (DataprojectNG, 2025).

The outdated systems also make the process of moving to cloud-based storage in Nigerian organisations difficult. Most organisations are still using old systems that are not readily compatible with the new cloud systems. The process of migrating the data in the legacy system to the cloud can oftentimes be associated with the need to make the technical changes to a significant extent, restructure the data and reengineer the procedures. These issues raise the complexity and risk of adopting clouds, especially for organisations with low technical capacity. Nevertheless, there is growing evidence that cloud-based storage systems can significantly enhance data protection and organisational resilience when properly implemented. Cloud service providers often offer advanced security features such as encryption, multi-factor authentication, automated backups, and disaster recovery mechanisms that surpass the capabilities of many on-premises systems. In a country like Nigeria, where

organisations frequently face power outages, hardware failures, and environmental risks, cloud-based storage systems can improve business continuity and reduce the risk of data loss.

In the education and public service sectors, emerging studies indicate gradual improvement in awareness and adoption of cloud technologies, driven by the need for efficient data management and digital service delivery. These developments suggest that cloud-based storage systems have the potential to play a transformative role in Nigerian organisations if challenges related to infrastructure, regulation, skills, and trust are adequately addressed. In view of the increasing dependence on digital data and the rising threat of cyber insecurity, examining cloud-based storage systems and effective data protection in Nigerian organisations is both timely and necessary. Such a study provides valuable insights into the extent of cloud adoption, the effectiveness of existing data protection measures, and the challenges organisations face in securing data in cloud environments. Ultimately, understanding these dynamics can inform policy formulation, organisational decision-making, and the development of strategies aimed at enhancing data protection and promoting secure digital transformation in Nigeria.

However, the following research questions guide the study:

1. What is the effect of cloud-based storage systems on data protection in Nigerian organisations?
2. What challenges do Nigerian organisations face in ensuring effective data protection when using cloud-based storage systems?

2. CONCEPTUAL REVIEW

2.1. CONCEPTUAL REVIEW OF CLOUD-BASED STORAGE SYSTEMS

Cloud computing includes cloud-based storage as an essential part of the system, which allows organisations to store, manage, and access data via remote servers, which are internet-based and not local or premise-based. Mell and Grance (2011) have defined cloud computing as a model where networking can be easily accessed on demand to a shared pool of configurable computing resources like networks, servers, storage, applications, and services. The cloud-based storage system follows this paradigm in that it is built with a scalable type of storage facility that can be accessed at any time or place as long as there is an internet connection.

There are three service models of cloud storage systems, which include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Under IaaS, organisations lease virtual storage and computing capabilities, which enables them to have more control over the data and security settings. PaaS offers the ability to create and run applications without the burden of managing the infrastructure, whereas SaaS offers fully managed applications in which the storage and security are managed by the service provider (Buyya et al., 2013). The models offer different degrees of flexibility, cost-effectiveness, and joint responsibility in the aspect of security between the provider and the user organisation.

Cloud-based storage systems are currently becoming the sock of the wool in Nigerian organisations owing to the fact that, in these entities, capital expenditure on hardware is minimised, the cost of maintenance and increase in the accessibility of data is also enhanced. The challenges that many organisations face include limited office space for servers, unreliable power supply, and excessive prices of IT infrastructure. The cloud storage can utilize the alternative option of offloading infrastructure management tasks to service providers so that organisations can concentrate on business operations instead of maintaining technical infrastructure (Owoseni et al., 2025).

Although these are the benefits, cloud-based storage systems also present issues related to ownership of data, control, and reliance on external service providers. Data availability, system availability, and security are the issues that organisations need to consider when relying on the vendors of cloud services. This dependence casts some very important doubts regarding trust, transparency, and accountability, particularly in developing countries such as Nigeria, where regulation and enforcement measures are still developing.

2.2. CONCEPT OF DATA PROTECTION AND INFORMATION SECURITY

Data protection can be defined as the set of procedures, policies, and technologies that are used to protect data against authorised access, misuse, loss, or destruction across its lifecycle. It includes information security elements such as confidentiality, integrity, and availability, also referred to as the CIA triad, which are the basis of information security (Whitman and Mattord, 2018). Confidentiality refers to the ability of data to be accessed by authorised personnel, integrity refers to the ability of data to be correct and free of corruption, and availability refers to the extent of data being available whenever it is required.

Data protection in organisations is essential because the information processed in organisations is sensitive, such as personal data, financial records, intellectual property, and operational information. Digitalisation has amplified the amount of data and vulnerability to cybercrime, and thus, organisations worldwide have made data protection a strategic priority in their operations. In cloud environments, data protection is even more complicated since only data is stored beyond the physical limits of the organisation, and it may be in more than one geographical location.

The data protection in cloud-based storage systems is dependent on technical and organisational measures. Some of the technical measures are encryption and firewalls, intrusion detection systems, access controls, and multi-factor authentication. Some of the organisational measures are to protect data policies, train employees, plan incident response planning, and monitor compliance (Clarke and Knake, 2010). The solution to these measures is the extent to which organisations incorporate them into their day-to-day procedures and governance systems. Data protection awareness in Nigeria has been enhanced as a result of the establishment of a new regulation, which is the Nigeria Data Protection Regulation (NDPR). Nevertheless, the practice is not uniform in organisations. Most organisations do not have policies on data protection or do not properly implement the ones they have, which exposes them to data breaches and regulatory non-compliance (Garga & Sadiq, 2025).

2.3. CLOUD-BASED STORAGE SYSTEMS AND DATA PROTECTION PRACTICES

There are a few security features provided by a cloud-based storage system that can be used to provide better protection to data if they are implemented effectively. Cloud service providers usually spend a lot on sophisticated security tools, such as encryption of data at rest, in transit, automated backup tools, backup recovery tools, and system monitoring. Such functionalities usually surpass the protection of the traditional on-premise systems, especially those that have a small IT budget (Armbrust et al., 2010).

One of the most important data protection mechanisms of cloud storage is encryption. It makes sure that the data is readable only by authorised users, even in case of a breach. The access controls also ensure that only users authorized to see or manipulate data are granted access to those resources, and audit logs also enable users to understand what happens in the system, which increases accountability and traceability. Backup and redundancy are both available to ensure that data is not lost due to system failure, cyberattack, or natural disasters.

But the success of such security mechanisms is highly determined by the way organisations set up and manage their cloud environments. One of the most common causes of cloud data breach in the world is misconfigurations, weak passwords, and ineffective access management. Poorly configured cloud systems are a common problem in Nigerian organisations, as limited technical knowledge is used to improperly set up cloud systems, thereby compromising the security advantages of cloud service providers (Disciplines.ng, 2024).

A second crucial concern is that of shared responsibility for cloud security. Although cloud service providers secure the underlying infrastructure, the user organisations secure their data, access controls, and applications. Nigerian organisations have a false understanding of this model because they believe that all issues of security are handled by the cloud providers. This illusion adds to the danger of data being exposed and compromises the organisational responsibility in data security.

2.4. REGULATORY AND LEGAL FRAMEWORK FOR DATA PROTECTION IN NIGERIA

In cloud-based storage systems, the environment of regulation is critical in influencing data protection practice. The main legal framework used in Nigeria in the curbing and transfer of personal information is the Nigeria Data Protection Regulation (NDPR). The regulation obliges the organisations to take appropriate technical and organisational precautions to secure the data and accountability in the performance of the third-party processors, such as cloud service providers. The existence of NDPR compliance both offers opportunities and challenges to organisations in Nigeria that have their cloud-based storage systems. On one hand, the regulation will ensure responsible data management and will pressurise organisations to engage in more powerful security practices. Conversely, compliance may also be challenging because of less regulatory guidance, insufficient enforcement systems, and insensitivity of organisations, especially SMEs (Bakare, 2020).

Cloud computing further complicates regulatory compliance due to cross-border data transfer. Data stored in cloud environments may reside on servers located outside Nigeria, subjecting it to foreign legal jurisdictions. This raises concerns about data sovereignty, legal accountability, and the ability of Nigerian authorities to enforce data protection standards in the event of breaches. Organisations must therefore carefully assess cloud providers' data residency policies and contractual obligations to ensure compliance with national regulations. Public sector organisations face additional challenges due to bureaucratic structures, slow decision-making processes, and limited funding for ICT projects. These factors often delay the adoption of cloud-based storage systems and the implementation of effective data protection measures, despite the growing need for secure and efficient data management in government institutions.

3. THEORETICAL REVIEW: SYSTEMS THEORY

The paper will be based on the Systems Theory that offers a valuable guide to the impact of cloud-based storage systems on data security within the context of Nigerian organisations. The Systems Theory is a theory that was initially formulated by Ludwig von Bertalanffy, and it considers an organisation as an open system whose elements are interdependent and are related to each other in order to work towards achieving shared goals (Bertalanffy, 1968; Scott, 2003). This theory states that the change in one aspect of the system is bound to influence other aspects, and the effectiveness of organisations is determined by the effectiveness of interactions and functioning of different components of the system.

When applied to the cloud-based storage system, Systems Theory can be used to clarify that the issue of data protection does not depend entirely on technology but on the interplay of several organisational factors. Such aspects are technological infrastructure, human resources, organisational policies, regulatory frameworks, and external service providers (Whitman and Mattord, 2018). Cloud-based storage systems are a subsystem that falls under the umbrella of organisational information systems, and their ability to secure information is pegged to their capacity to integrate with other subsystems such as cybersecurity governance, employee behaviour, and management support (Clarke and Kanake, 2010).

In a Systems Theory approach, balance and coordination between components of the system would be necessary to ensure the good protection of data in cloud environments. As an illustration, despite the fact that an organisation implements a very secure cloud-based platform to store data, poor internal policies, lack of adequate staff training, or ineffective access control systems can lead to breaches of data security (Armbrust et al., 2010). This is indicative of the principle of systems, which states that the behaviour of the entire system is determined by the interplay of its components, not by the effectiveness of any single component. Systems Theory in Nigerian organisations is very applicable as the operating environment is quite complex with infrastructural problems, regulatory barriers, and scarce technical capacity. According to the theory, cloud-based storage systems cannot ensure successful data protection without the supporting systems, including the presence of reliable internet connectivity, competent staff, the existence of a data protection policy, and compliance mechanisms (Owoseni et al., 2025). Any vulnerability of these interrelated components will disrupt the whole data protection mechanism.

Besides, the Systems Theory focuses on the feedback mechanisms, which play a crucial role in the constant improvement. Feedback in cloud-based storage systems may be comprised of a security audit, system monitoring report, incident response assessment, and compliance assessment (Mell and Grance, 2011). Such feedback mechanisms enable organisations to establish areas of weakness, modify security controls, and enhance data protection practices over a period of time. In short, Systems Theory is valuable for careful consideration of cloud-based storage systems and efficient data protection in Nigerian organisations. It points out that the protection of data is a joint effort of technology, people, and organisations. Using this theory, the paper highlights the importance of a comprehensive approach to cloud adoption, as the implementation of the technology should be supported by robust governance, professional skills, and consistent system assessment to ensure successful data protection (Bakare, 2020; Whitman and Mattord, 2018).

4. EMPIRICAL LITERATURE

There has been mixed empirical research on cloud computing and data protection. In some of the studies, there are findings that cloud-based storage systems are essential in enhancing the data security and operational efficiency of organisations in case they apply the relevant security practices (Armbrust et al., 2010). Others point out that ineffective governance, lack of skills, and enforcement of regulations invalidate the efficacy of cloud security measures, especially in emerging economies.

Research carried out in organisations in Nigeria indicates that organisations are becoming more aware of cloud computing, but the adoption is moderate. The studies show that perceived security risks, uncertainties of the regulations, and infrastructural constraints are some of the most important factors affecting the decision to adopt the cloud (Bakare, 2020). According to other studies, organisations with a high level of employee training and data governance frameworks report high levels of data protection among cloud environments (Garga & Sadiq, 2025).

Nevertheless, the current research is largely generalised in terms of cloud adoption or organisational performance, and there is not much particular attention to discussing the correlation of cloud-based storage systems and efficient data protection in the environment of Nigerian organisations. This shortcoming underscores the need for additional empirical research to provide context-dependent information and policy-based recommendations.

5. EFFECT OF CLOUD-BASED STORAGE SYSTEMS ON DATA PROTECTION IN NIGERIAN ORGANISATIONS

Protection of data by cloud-based storage systems has been a subject of numerous debates in the information systems and cybersecurity literature. Cloud-based storage systems are designed to help organisations store, manage, and protect data by leveraging remote servers, robust security architectures, and automated management systems. There is a general consensus among scholars that cloud-based storage systems, when appropriately adopted, can significantly enhance the results of data protection as opposed to the on-premises systems (Armbrust et al., 2010).

Enhanced data backup and availability have been noted to be one of the significant impacts of cloud-based storage systems on data protection. Cloud service providers have automated data backup, redundancy, and disaster recovery systems that help organisations to prevent the loss of their data in case of a hardware failure or power interruption, or natural disasters. Cloud storage is more secure in the case of unstable electricity supply and system failures in organisations, which occur quite often in the Nigerian context and need more reliable data integrity and continuity (Owoseni et al., 2025). This will increase the availability of data and decrease the chances of a complete loss of data.

Cloud-based storage systems also enhance data confidentiality by leveraging advanced security technologies, including encryption, identity management, and access control. When using data encryption, the information stored within the system cannot be read by a non-authorised user, even in the case of a security breach. Research has shown that most cloud providers apply encryption standards more advanced than those used by small and medium-sized organisations that operate on-premises servers (Clarke and Kanke, 2010). Consequently, the ability to experience increased data confidentiality is particularly experienced in the Nigerian organisations that incorporate the use of cloud storage, especially when dealing with sensitive customer or employee data.

Data protection is another notable impact of the cloud-based storage systems on data protection, as it improves monitoring and threat detection. Cloud environments usually involve the consistent monitoring of the systems, security upkeep automation, and intrusion detection systems. The features allow detecting and eliminating cyber threats at an early stage. Cloud-based monitoring tools can be used to address internal deficits in Nigeria-based organisations, where cybersecurity expertise can be limited by delivering real-time alerts and security analytics (Whitman and Mattord, 2018).

The benefits of cloud-based storage systems, as far as data protection is concerned, are not automatic, however. The shared responsibility model of cloud security entails user organisations controlling access rights, user authentication policy, and data governance policy. It has been demonstrated in literature that organisations that do not understand or apply their security responsibilities adequately can experience breaches of their data even when they have applied cloud services (Mell & Grance, 2011). In Nigeria, poor security governance and technical competence tend to reduce the efficiency of cloud-based data protection.

More so, cloud-based storage systems affect regulatory compliance and accountability. Data protection requirements can be backed by the use of audit trails, access logs, and data classification tools to comply with the regulations of data protection when using cloud services. The Nigeria Data Protection Regulation (NDPR) can be easier to align with by Nigerian organisations that have compliant cloud providers. Nonetheless, data sovereignty and cross-border data storage raise concerns that could complicate the regulatory process and create concerns about the legal responsibility of such data in case of breaches (Bakare, 2020).

On the whole, the literature indicates that cloud-based storage is associated with an overall positive impact on data protection in Nigerian organisations. These systems increase the availability of data, confidentiality, and integrity, where these are backed up by the right organisational policies, employee knowledge, and regulatory adherence. In the absence of supporting factors, however, the advantages of cloud-based storage in data protection can be significantly reduced.

6. CHALLENGES INVOLVED IN THE PROCESS OF EFFECTIVE DATA PROTECTION BY MEANS OF CLOUD-BASED STORAGE SYSTEMS.

Although cloud-based storage systems offer significant advantages, Nigerian organisations face several challenges when implementing efficient data protection. Poor ICT infrastructure is one of the problems most frequently mentioned in the literature. The cloud-based storage systems are heavily reliant on internet connectivity and electricity availability. Network outages and power interruptions are common in Nigeria and make it difficult to access cloud services continuously and to build trust in their reliability, particularly for important organisational information (Owoseni et al., 2025).

Lack of technical knowledge and cyber skills in organisations is yet another significant challenge. To ensure data security in the cloud, one must be familiar with cloud architecture, encryption guidelines, access control measures, and incident response protocols. Nigeria does not have a large number of IT-trained personnel who can handle these technical requirements. Consequently, cloud systems tend to be configured poorly, which exposes data to unauthorised access and malconfigurations as well as cyberattacks (Disciplines.ng, 2024).

Employee behaviour and organisational awareness are also major issues for the protection of data in cloud environments. It has been witnessed in literature that human error is one of the most dominant causes of data breaches across the world. Poor employee training in cloud security practices in Nigerian organisations exposes employees to weak passwords, phishing, and accidental data exposure. The effectiveness of cloud-based data protection is severely compromised without ongoing staff sensitisation and security awareness programmes (Whitman and Mattord, 2018).

Data protection is also complicated by regulatory and legal issues. Even though the Nigeria Data Protection Regulation (NDPR) offers a framework of data protection, most organisations have difficulties in compliance because of poor knowledge of the nature of regulatory requirements and the lack of learning and effective enforcement mechanisms. Cloud computing also becomes a legal issue due to the fact that data can be located somewhere beyond Nigeria, which poses the problem of data sovereignty and legal control. Cloud service agreements that can sufficiently tackle the issue of data protection and liability are not always negotiated by organisations that are knowledgeable of the legal specifics of the matter (Bakare, 2020).

Effective data protection in cloud-based storage systems is also influenced by cost-related factors. Whereas cloud services save on long-term infrastructure costs, costs of secure migration, subscription costs, compliance audit, and employee training can be high. In particular, small and medium-sized businesses can make cost-saving goals their top priority at the expense of strong security settings, thereby making their data more vulnerable to risks (DataprojectNG, 2025).

Lastly, resistance to change in organisations is also a major challenge. A lack of confidence in the security of third-party service providers, fear of data loss, and management scepticism tend to slow cloud adoption or lead to the implementation of only some aspects of cloud services. This kind of resistance narrows down the scope of implementing the holistic approach to data protection and denies organisations an opportunity to enjoy the full benefits of cloud-based data storage systems in terms of security.

Overall, the literature shows that several interrelated factors make it difficult to ensure the effectiveness of data protection in Nigerian organisations that use cloud-based storage systems. The problems can only be resolved through better infrastructure, skill development, clarity in regulations, organisational consciousness, and management's dedication to adopting the cloud.

7. CONCLUSION

This paper has discussed cloud-based storage systems and efficient data protection within Nigerian organisations, with specific reference to the impact of cloud-based storage on data protection and to how organisations struggle to protect their data. Based on the available literature, it is clear that cloud-based storage systems are an important technological development that can transform data management practices in organisations in Nigeria. This research concludes that cloud-based storage systems can be used to enhance data protection by ensuring availability, integrity, confidentiality, and resilience. Automated backups, encryption, access controls, disaster recovery, and a constantly monitored system are among the features provided by cloud service providers, and these can walk on water when it comes to data security compared to traditional on-premises storage systems. The advantages will be especially valuable within the Nigerian environment, where organisations usually face a problem of unreliable power supply, inadequate ICT infrastructure, and excessive expenses to support physical servers.

The research, however, also finds that cloud-based storage systems are effective in securing organisations data; this is mainly because of their effectiveness in implementation and management. Among the challenges that compromise the data protection advantages of cloud computing are: lack of technical skills and knowledge on the shared responsibility model, ineffective organisational data governance policies, and staff lack of awareness. Moreover, the subject of regulatory and legal issues, such as adherence to the Nigeria Data Protection Regulation (NDPR) and the problem of data sovereignty, has also had an impact on organisational trust in cloud-based solutions. On the whole, the paper confirms that although cloud-based storage systems have a significant potential in enhancing data protection in Nigerian organisations, it is only possible to realise the potential fully in the case infrastructural, organisational, regulatory, and human capacity issues are properly resolved. Cloud adoption can increase an organisation's vulnerability to new security threats rather than mitigating them, unless specific efforts are made to develop more robust data protection practices.

8. RECOMMENDATIONS

Going by the results and conclusions of this study, the following are the recommendations that can be made to improve the efficient protection of data using cloud-based storage systems in Nigerian organisations:

1. Comprehensive policies on data protection and cloud security should be formulated and adopted by Nigerian organisations. These policies ought to be explicit in covering data classification, data access control processes, encryption requirements, backup policies, and the response mechanisms of incidents. Clarity of policies will be used to control the behaviour of the employees and to make sure that there is uniformity in data protection practices within the organisation.
2. Organisations are encouraged to invest in frequent training programs for IT personnel and other employees on cloud computing, cybersecurity, and data protection best practices. Enhancing the competence of the staff will decrease human error, improve the correct setup of the cloud systems, and improve the organisational capability to take appropriate action during data security incidents.
3. Nigerian organisations must be keen on using cloud service providers who meet international security standards and data protection requirements set by the Nigerian government. Data protection responsibilities, data residency requirements, breach notification procedures, and liability clauses should be outlined in service-level agreements (SLAs) to protect the organisation's interests.
4. Cloud-based data storage systems should be adhered to by organisations, and in particular, SMEs and government facilities, but with non-critical types of data, and by enhancing security measures. This incremental process will minimise risks, instill confidence in cloud systems, and enable organisations to enhance their capacity to protect data over time.

9. IMPLICATIONS OF THE STUDY

This study has a number of implications for organisations and practitioners in Nigeria. For Nigerian organisations, the current study shows the need to view cloud-based storage systems not only as tools that save costs but also as strategic resources that must be governed and managed for security. Organisations that do not focus on data protection can be prone to data breaches, financial losses, reputational damage, and even legal ramifications. The paper has thus highlighted the necessity to get the management to commit itself to cloud adoption and keep on enhancing data protection practices. The study provides ICT managers and cybersecurity practitioners with an idea of the real-life challenges of securing cloud-based storage systems. It emphasizes the importance of system configuration, continuous monitoring, employee education, and cooperation with cloud service providers to ensure efficient data protection.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010, doi: https://doi.org/10.1145/1721654.1721672.

[2] A. Bakare, Cloud computing adoption in Nigerian government organisations: The role of perceived security risks, Doctoral dissertation, Walden University, 2020.

[3] R. A. Clarke and R. Knake, Cyber War : the Next Threat to National Security and What to Do About It. New York: Harpercollins E-Books, 2010.

[4] L. von Bertalanffy, General System Theory: Foundations, Development, Applications. New York: Braziller, 1968.

[5] Rajkumar Buyya, J. Broberg, and A. M. Goscinski, Cloud Computing. John Wiley & Sons, 2010.

[6] DataprojectNG, The impact of cloud computing adoption on business efficiency in Nigeria, DataprojectNG Research Publications, 2025. [Online]. Available: https://www.dataprojectng.com/project/32328/The%20Impact%20of%20Cloud%20Computing%20Adoption%20on%20Business%20Efficiency%20in%20Nigeria

[7] Cloud Adoption in Nigeria: Opportunities, Challenges & Success Stories, PlanetWeb solutions, 2024. [Online]. Available: https://planetweb.ng/cloud-adoption-in-nigeria/

[8] A. Garga, and A. A. Sadiq, "Data protection and cybersecurity challenges in cloud computing environments in Nigeria," International Journal of Advanced Technology and Engineering Studies, vol. 9, no. 2, pp. 45–58, 2025.

[9] M. Marvis, and O. Emmanuel, "Cloud computing technology: A secured and cost-effective data storage system," International Journal of Engineering Research & Technology, vol. 3, no. 6, pp. 1120–1125, 2014.

[10] P. Mell, and T. Grance, The NIST definition of cloud computing (Special Publication 800-145). National Institute of Standards and Technology, 2011.

[11] A.O. Owoseni, T. O.Adeyemi, and M.O. Lawal, "Cloud computing adoption and organisational performance in Nigeria," Nigerian Journal of Management Sciences, vol. 6, no. 1, pp. 23–39, 2025.

[12] W.R. Scott, Organizations: Rational, natural, and open systems, 5th ed, Prentice Hall, 2003.

[13] M. E. Whitman and H. J. Mattord, Principles of information security. Boston, Mass.: Thomson Course Technology, 2009.