International Journal of Advanced Technology in Engineering and Science
Vol. No. 13, Issue No. 07, July 2025
www.ijates.com
ijates
ISSN 2348 - 7550

# A STUDY OF PRIVACY AND SECURITY ISSUES IN ADOPTION, SPI SERVICES, DEPLOYMENT MODELS AND TECHNOLOGIES OF CLOUD COMPUTING: A NIGERIAN PERSPECTIVE

**Faisal Bala Garga & Suleiman Muhammed Sadiq**

*Department of Information Technology, Nigerian Army University Biu*

**Abstract**

*Cloud computing has emerged as a transformative technology that offers scalable, flexible, and cost-effective IT resources delivered over the internet. It enables individuals and organizations to access computing power, storage, and applications on demand, significantly improving data management and operational efficiency. In Nigeria, both government and enterprises increasingly recognize cloud computing's potential, yet data privacy and security concerns hinder widespread adoption. This study explores these security challenges within the Nigerian context, focusing on SPI (Software, Platform, Infrastructure) service models, deployment models (public, private, community, hybrid), and enabling technologies. Through a comprehensive literature review, threat analysis, and data collection from Nigerian cloud service providers and end-users, the research identifies gaps in existing security frameworks. It proposes a security control-based framework specifically designed to address these gaps and enhance trust. A prototype implementation demonstrates a practical solution with encryption, access control, and audit mechanisms. Findings offer valuable insights for Nigerian policymakers, cloud service providers, and organizations to enhance cloud adoption securely, while anticipating broader implications for other emerging markets.*

***Keywords:*** *Cloud Computing, Security, Privacy, SPI Models, Deployment Models, Framework, Nigeria, Cloud Adoption, Data Protection*

## INTRODUCTION

With the rapid growth of technology, the landscape of data storage and computing has significantly evolved. One of the most transformative innovations in this area is Cloud Computing. This technology offers scalable and cost-effective IT resources that can be accessed over the internet. It promises flexibility, operational efficiency, and dynamic resource allocation for both individuals and organizations.

However, despite its many advantages, cloud computing faces significant security and privacy concerns, which have slowed its adoption, especially in sensitive environments like finance, healthcare, and government. Users often express fears related to data breaches, unauthorized access, compliance issues, and trust in cloud service providers.

According to the National Institute of Standards and Technology (NIST, 2015), cloud computing is: "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,

networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud services are typically categorized into three service models collectively known as SPI:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

These services are deployed through four deployment models:

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

These models are supported by a wide range of technologies and infrastructures that make cloud computing possible (Bhargava, 2012).

Although cloud computing simplifies access to computing resources and offers benefits like on-demand self-service, broad network access, and pay-as-you-go pricing, data security remains a major obstacle to its wider adoption. The dispersed nature of cloud environments—where data resides across multiple devices, networks, and locations—creates challenges in securing and monitoring sensitive information (Rabi et al., 2011).

To earn user trust and improve adoption, cloud security must be strengthened. Users need assurance that their data is protected from external threats and unauthorized internal access.

## Problem Statement

The core challenge addressed in this research is the lack of strong security controls in cloud computing platforms, which hinders user trust and adoption. Although cloud computing provides a flexible and cost-effective alternative to traditional IT infrastructure, the growing number of cyber threats and data leaks continues to discourage organizations from migrating fully to the cloud.

## Research Objectives

This study is aimed at the following objectives:

1. To evaluate security threats in cloud computing, especially concerning SPI models and deployment approaches.
2. To recommend effective security enhancement methods in SPI models and cloud deployment systems.
3. To propose a cloud security control-based framework for secure data storage and user privacy.
4. To develop a prototype based on the proposed framework.
5. To analyze how the proposed security model can improve cloud adoption among organizations and individuals.

## Research Questions

To guide this research, the following key questions are addressed:

1. Is cloud computing effective in the context of big data storage and management?
2. How can cloud security controls mitigate risks such as data loss, unauthorized access, privacy violations, and malware attacks?
3. How do existing SPI models and deployment models influence the adoption of cloud computing?
4. How effective are the recommended security methods in enhancing adoption of cloud computing?
5. Is there alignment or disparity in cloud security concerns between cloud providers and cloud users?

### Significance of the Study

This study will contribute by:

- Offering a comprehensive understanding of security and privacy issues in cloud computing.
- Developing a security control-based framework to reduce data breaches and enhance trust.
- Providing a prototype to validate the practical application of the proposed framework.
- Helping both individuals and organizations make informed decisions on cloud adoption.
- Facilitating collaboration between cloud service providers and users to jointly manage risks.

The outcomes will support policy makers, researchers, IT administrators, and cloud developers in addressing cloud adoption barriers.

### Delimitations of the Study

This research is limited in scope to:

- Cloud Service Providers (CSPs) and Cloud End-Users (CEUs)
- Experts from selected organizations and institutions
- Geographical focus on selected regions within Nigeria

While the study will include the development of a prototype, the full implementation of the complete framework may be extended to future research.

### Conceptual Definition: Cloud Computing (NIST)

Cloud computing, as defined by NIST, is: A model that enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network, server, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

## COMPREHENSIVE LITERATURE REVIEW

This chapter presents a comprehensive review of empirical and conceptual literature relevant to the research topic—Cloud Computing, SPI Models, Deployment Models, and Associated Technologies. The aim is to develop a clear understanding of the key concepts, current trends, and research gaps in cloud computing, particularly in relation to privacy and security issues.

To systematically address some of the study's objectives and research questions, the review is organized under the following key thematic areas:

### History and Theory of Cloud Computing

The evolution of cloud computing has its roots in the early developments of computing and data networking. According to Venkatesan Prabu (2015), the origin of cloud computing can be traced back to 1941 with the invention of the first general-purpose electronic computer. Over time, computing evolved into networked systems, leading to data sharing and the client-server architecture in 1976. By 1983, the idea of renting not only storage but also full server environments marked the beginning of the cloud era. In the 2000s, commercial cloud services became accessible via the internet, enabling users to access computing resources without managing the underlying infrastructure. Cloud computing has since revolutionized IT services, but security remains a critical concern.

## RESEARCH METHODOLOGY

Software design involves principles and practices for building high-quality systems. It is a structured process that ensures the proper translation of user requirements into effective system designs.

Software design is defined as: A systematic, intelligent process in which designers generate, evaluate, and specify concepts for a software system whose structure and function achieve clients' objectives or users' needs, while satisfying a specified set of constraints.

In this study, the design process focuses on creating a cloud security framework that answers the research questions and meets project requirements. Key considerations include:

- Managing complexity through separation of concerns;
- Producing abstract representations of design decisions;
- Defining terms unambiguously;
- Establishing guided pathways for user tasks.

### Design Process in Agile Development

Traditional software development follows structured phases, producing models that guide implementation. However, Agile methods view design as iterative and emergent. In Agile:

- Only coding, testing, and refactoring reveal the true design;
- Evolutionary design adapts during development but can result in poor structure if unmanaged;
- Rapid technology changes and unforeseen requirements challenge initial designs.

This study adopts a hybrid design approach, balancing planned architecture with Agile adaptability.

### Architecture Design

Architecture is a foundational element in software development. According to TOGAF, it is:

1. A formal system description or detailed component-level plan;
2. The structure of components and their interactions, along with principles governing their evolution.

This project uses architectural envisioning to guide design decisions and ensure alignment with objectives. A well-defined architecture helps decompose the system into functional modules and supports the separation of concerns.

### Software Architecture

Software architecture defines structured solutions that meet technical and operational needs while optimizing qualities such as performance and security. Key aspects include:

- System decomposition into modules;
- Difficult-to-reverse design decisions;
- Multiple architectural layers;
- Focus on elements with long-term significance.

The architectural model supports the implementation of a cloud security prototype, addressing data protection, access control, encryption, and user privacy while remaining adaptable for future enhancements.

## DATA PRESENTATION AND ANALYSIS

This chapter presents the results obtained from both the quantitative and qualitative research approaches employed in the study. Data was collected using structured questionnaires, interviews, and document reviews. The findings are analyzed and interpreted in relation to the research questions and objectives set out in Chapter One.

### Demographic Characteristics of Respondents

A total of 120 respondents were surveyed across various sectors including IT, education, healthcare, finance, and government. Participants included cloud service providers, IT professionals, academic researchers, and cloud end-users.

- **Gender Distribution:** 70% male, 30% female
- **Educational Background:** 60% postgraduate, 40% undergraduate
- **Years of Experience:** 40% (1–5 years), 35% (6–10 years), 25% (11+ years)

**Awareness and Adoption of Cloud Computing**

- 88% of respondents are aware of cloud computing.
- 67% use cloud services in their organizations.
- Major services used: SaaS (60%), IaaS (25%), PaaS (15%)

**Perceived Benefits of Cloud Computing**

Respondents identified the following as key benefits:

- 80%: Flexibility and scalability
- 72%: Cost reduction
- 68%: Ease of access and collaboration

**Challenges and Concerns in Cloud Computing Adoption**

Security and privacy concerns were the top obstacles reported:

- 76%: Data breaches and unauthorized access
- 60%: Lack of trust in service providers
- 52%: Regulatory and legal issues
- 45%: Poor infrastructure and internet reliability

### Evaluation of Security Practices in Use

The following security measures were commonly adopted:

- 70%: Password protection and access control
- 65%: Encryption of sensitive data
- 45%: Regular backups and disaster recovery
- 40%: Use of firewalls and antivirus tools

However, only 28% of respondents reported using comprehensive security frameworks like ISO/IEC 27001 or NIST guidelines.

### Framework Validation Feedback

Prototype of the proposed security control-based framework was demonstrated to select organizations:

- 85% found the proposed model effective in enhancing trust.
- 78% appreciated the access control and encryption modules.
- 70% agreed the model could be adopted in real-world deployment with minimal adjustments.

**Summary of Findings**: The data analysis confirms:

- High awareness but moderate adoption of cloud computing in Nigeria.
- Security remains the most significant barrier to adoption.
- Existing security practices are basic and lack advanced threat detection.
- The proposed framework is perceived as a viable solution to close the adoption

## DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

This study set out to investigate privacy and security challenges affecting the adoption of cloud computing services in Nigeria, focusing on SPI service models and deployment frameworks. The analysis from Chapter Four revealed several key insights:

- **Awareness and Adoption:** The high awareness (88%) about cloud computing indicates a good understanding among IT professionals and organizations. However, adoption is moderate (67%), constrained primarily by security and privacy concerns.
- **Security Concerns:** Data breaches, unauthorized access, and lack of trust in providers remain significant barriers. These findings align with global trends but are accentuated by Nigeria's developing cybersecurity infrastructure and legal frameworks.
- **Current Security Practices:** Organizations mainly rely on basic security mechanisms such as password protection and encryption. Few adopt comprehensive standards like ISO 27001 or NIST, signaling a gap in best practices implementation.
- **Framework Effectiveness:** The proposed security control-based framework was well received by stakeholders, showing promise in improving trust and secure cloud usage. The framework's modular design supports encryption, access control, and audit mechanisms critical for data protection.

The study confirms that security is pivotal in cloud adoption decisions in Nigeria, and tailored security frameworks can substantially mitigate risks and increase confidence among users.

## Conclusion

Cloud computing offers transformative opportunities for Nigeria's digital economy, improving scalability, cost-efficiency, and operational agility. Yet, security challenges, particularly regarding data privacy and trust, have slowed its full adoption.

This research successfully identified the key security risks in SPI and deployment models and developed a context-specific security framework. The prototype demonstrated practical feasibility in addressing these challenges, making it a valuable tool for Nigerian enterprises and cloud service providers.

To foster widespread cloud adoption, continuous improvements in security policies, infrastructure, and awareness are essential. Collaboration between government, industry, and academia will be crucial to strengthen legal frameworks and build user confidence.

## Recommendations

Based on the findings, the study recommends: **doption of Robust Security Frameworks:** Organizations should implement comprehensive frameworks like ISO/IEC 27001 and integrate encryption, access control, and continuous monitoring.

1. **Government Policy and Regulation:** Nigerian policymakers need to enforce data protection laws and cybersecurity standards that address cloud-specific risks.
2. **Capacity Building and Awareness:** Continuous training and awareness campaigns should be conducted for IT professionals and end-users regarding cloud security best practices.
3. **Infrastructure Improvement:** Investments in reliable internet connectivity and cybersecurity infrastructure are critical to support secure cloud services.
4. **Collaboration among Stakeholders:** Cloud service providers, users, and regulators should establish forums for sharing threat intelligence and jointly improving security measures.
5. **Further Research:** Future studies could focus on refining the proposed framework, exploring emerging threats like insider risks, and evaluating long-term adoption trends.

## Limitations of the Study

While this research provides valuable insights, limitations include:

- Geographical focus limited to selected Nigerian regions, possibly limiting generalizability.
- Prototype implementation scope was limited; full-scale deployment is recommended for deeper evaluation.
- Rapid evolution of cloud technologies means emerging threats could change the security landscape quickly.

**Areas for Future Research**

- Development of automated security tools tailored for Nigerian cloud environments.
- Investigation of cloud adoption in small and medium enterprises (SMEs).
- Impact assessment of international data privacy regulations (like GDPR) on Nigerian cloud users.

ijates
ISSN 2348 - 7550

## References


- Bhargava, B. (2012). *Cloud Computing: Services and Deployment Models*.
- National Institute of Standards and Technology (NIST). (2015). *The NIST Definition of Cloud Computing*.
- Rabi, P. P., et al. (2011). *Data Security and Privacy in Cloud Computing*.
- Prabu, V. (2015). *The History and Evolution of Cloud Computing*.
- The Open Group. (n.d.). *TOGAF® Standard, Version 9.2*.