



**"INFORMATION TECHNOLOGY, THE PATHWAY TO THE CLOUD:
DEMYSTIFYING THE FEARS OF 'GOING CLOUDY' WITHIN
THE NIGERIAN DIGITAL LANDSCAPE"**



**INAUGURAL
LECTURE**
OF SOUTHERN DELTA
UNIVERSITY,
OZORO, NIGERIA.



TO BE DELIVERED BY

**ENGR. PROFESSOR
PASCHAL UCHENNA
CHINEDU**

PROFESSOR OF INFORMATION SYSTEMS AND TECHNOLOGY
ND (Owerri) HND (Auchi); PGD (FUTO); M.Sc. (Northumbria, UK); Ph.D. (FUTO)

Printed By:
SOUTHERN DELTA UNIVERSITY PRESS, OZORO
@08038221708

PROFESSOR PASCHAL UCHENNA CHINEDU

6th Inaugural Lecture of Southern Delta University, Ozoro, Nigeria

**“INFORMATION TECHNOLOGY, THE
PATHWAY TO THE CLOUD: DEMYSTIFYING
THE FEARS OF ‘GOING CLOUDY’ WITHIN THE
NIGERIAN DIGITAL LANDSCAPE”**



By

ENGR. PROFESSOR PASCHAL UCHENNA CHINEDU,

**ND (Owerri) HND (Auchi); PGD (FUTO); M.Sc. (Northumbria,
UK); Ph.D. (FUTO)**

FNCS, FAAPM, MIET, MIEEE, MNSE, MCPN- CITP, R.ENG-COREN

Professor of Information Systems and Technology

Dean, Faculty of Computing

Tuesday, 18th August 2026

PROFESSOR PASCHAL UCHENNA CHINEDU

6th Inaugural Lecture of Southern Delta University, Ozoro, Nigeria



Copyright ©

Professor Paschal Uchenna Chinedu

All right reserved. No part of this book may be reproduced, stored in any retrieval system or by any means, photocopying, electronic, mechanical, recording or otherwise, without the prior permission of the author.

ISSN: 0794-1536

Printed by

Southern Delta University Press

@ 08038221708

DEDICATION

This Inaugural Lecture is dedicated to God Almighty for according to me the privilege to present the Sixth (6th) Inaugural Lecture of the prestigious Southern Delta University (SDU), Ozoro, Nigeria.

ABSTRACT

Mr. Vice Chancellor Sir, this inaugural lecture examines the journey of Information Technology from its centralized mainframe origins, through the era of distributed computing, and back again to today's cloud environment. It argues that cloud computing represents not just a technological shift but a fundamental transformation in how organizations access, manage, and secure their digital resources. Drawing on over a decade of research, survey data from 124 technology professionals and financial services stakeholders, and analysis of Nigeria's evolving policy landscape, the lecture identifies the anatomy of fear that has slowed cloud adoption in Nigeria, particularly around security, privacy, and loss of control. It demonstrates that while these concerns are valid, they are not insurmountable. The lecture presents the author's contributions to cloud security frameworks and encryption solutions, reviews recent Nigerian policies including the Nigeria Data Protection Act (2023) and the National Data Classification and Sovereignty Framework (2025), and projects significant economic impacts with potential GDP contributions of up to ₦30.2 trillion by 2033. The lecture concludes that Nigeria stands at a pivotal moment where embracing cloud computing is no longer optional but essential for competitiveness, and offers practical recommendations for stakeholders across government, industry, and academia to accelerate responsible cloud adoption while addressing legitimate security concerns.

Keywords: Cloud Computing, Information Technology, Cybersecurity, Digital Transformation, Nigeria, Data Privacy, Cloud Adoption, IT Policy

TABLE OF CONTENTS

Inner Page

Copyright Page

Dedication

Abstract

Table of Contents

Protocol

Preamble

1.0 Introduction

1.1 Computer Science, Information Technology and Information Systems

1.2 The Evolution to Cloud Computing (How Did We Get Here?)

1.3 The Pathway to the Cloud

1.4 The Mataphor of ‘Going Cloudy’

1.4.1 Key Aspects of the Metaphor

1.4.2 Examples of "Going Cloudy"

1.5 Problem Statement

1.6 Aim and Objectives

1.7 Scope

2.0 Understanding Cloud Computing

2.1 Cloud Computing Service Models

2.2 Cloud Computing Deployment Models

2.3 Essential Characteristics of Cloud Computing

2.4 Anatomy of Fear: Understanding Cloud Security Concerns

2.5 Cloud Computing Threat Model

2.6 Cloud Data Security: Concerns and Solutions

2.7 Nigeria-Specific Risk Analysis of Cloud Deployment and Service Models

3.0 Research Methodology

3.1 Research Approach and Design

3.2 Population and Sampling

3.3 Data Collection Instruments

3.4 Data Analysis Techniques

4.0 Findings and Discussions

- 4.1 Business and Security Benefits of Cloud Computing
- 4.2 Security and Privacy: The Main Obstacles
- 4.3 Mission-Critical Processes and Sensitive Data
- 4.4 Current Security Solution Implementation
- 4.5 Demystifying the Fears: Overcoming Barriers to Adoption
- 4.6 Nigeria's Policy Framework for Cloud Computing
- 4.7 Cloud Computing's Impact on Nigeria's Economy

5.0 My Contribution to Cloud Computing Research

- 5.1 Security of Cloud Virtualized Resource on a SaaS Encryption Solution (2018)
- 5.2 Optimizing a Cloud Model for Effective and Efficient Collaboration in a Virtual World (2018)
- 5.3 Secured Cloud-Based Framework for ICT Intensive Virtual Organisation (2018)

6.0 Conclusion and Recommendations

- 6.1 Conclusion
- 6.2 Recommendations

7.0 Acknowledgments

8.0 References

Appendix:

Past Inaugural Lectures and Dates

PROTOCOLS

The Vice-Chancellor
The Deputy Vice-Chancellor
The Provost
The Registrar
The Bursar
The University Librarian
Deans of Faculties and of Student Affairs
Directors
Professors
Heads of Department
Members of the Academia
Other Staff of the University
Royal fathers
My Lords, Spiritual and Temporal
Distinguished Invited Guests
Gentlemen of the Press
Great Students of SDU
Ladies and Gentlemen

PREAMBLE

Let me specially thank the Almighty God for my salvation and journey of faith in the place called Christ; and for making it possible for me to have this opportunity to deliver my inaugural lecture today before my respected colleagues, friends, relations and students.

My academic journey traversed Federal Polytechnic Auchi, Nigeria; Northumbria University, Newcastle upon Tyne, UK; Federal University of Technology, Owerri; Wellspring University, Benin City; Federal University Oye-Ekiti, Edo State University, Iyamho and now Southern Delta University, Ozoro, Delta State– Nigeria where my professorial rank to full chair was attained.

The digital and our able Vice-Chancellor, sir, it gives me great pleasure, privilege and honour to stand before you, your Management Team and this distinguished audience to deliver this 6th lecture, marking my inauguration as a Professor of Information Systems and Technology in the Faculty of Computing of this great and prestigious University – Southern Delta University, Ozoro. This Inaugural Lecture is the first both in the Faculty of Computing and in the Department of Information Systems and Technology. However, this is sixth to be given in Southern Delta University, Ozoro, Nigeria. To God be the glory. Again, I am indeed very grateful to the Vice-Chancellor Professor Sunny Awhefeada for the opportunity he has given me to deliver this lecture. Thank you, sir.

An inaugural lecture is a forum at which a professor gives an insight into his work, what he has been doing up to date, what contributions he has made to advance the frontiers of knowledge, the relevance of his work to society and to the improvement of the quality of life to humanity. Also, it affords him the opportunity to highlight his present research work. This event represents a landmark in the academic career of the lecturer.

In recent years, Information Technology (IT) has played a very important role in our daily lives. There are several areas within various disciplines where Information Technologies are applied extensively these days. These include its role or applications in homes, business, education, research organizations, medical field, industry, government, banks, entertainment, business, training, arts, science and engineering, etc. Further, computers and portable devices such as Smart phones are used more extensively than ever for tasks such as marketing, banking, investing, shopping and communicating. These trends are no doubt having more positive than negative impacts on our society and economy leading to the emerging digital transformation in our society today.

This inaugural lecture presents me a remarkable opportunity as a Professor of Information Systems and Technology to inform this audience, especially my colleagues at the university, and the public about the emerging Information Technology trends, progress, and achievements in my core area of research career which is Cloud Computing. Cloud computing is a major component and application of both Information Technology (IT) and the broader field of Information and Communications Technology (ICT). Thus, within this lecture, both terminologies would be used interchangeably to connote the same thing.

I am truly honoured by the management of this great citadel of learning, being offered this great privilege to present the 6th Inaugural Lecture titled- “INFORMATION TECHNOLOGY, THE PATHWAY TO THE CLOUD: DEMYSTIFYING THE FEARS OF “GOING CLOUDY” WITHIN THE NIGERIAN DIGITAL LANDSCAPE”. My choice of this topic was to enable me to introduce, discuss, and analyze my scholarly achievements in my chosen area of specialty- Cloud computing. Also, it will be my pleasure to present a few of my contributions to learning and research in the field of Cloud Computing.

This lecture will be presented using simple language and concepts that will be understood by everyone here in attendance today and my future readers of this lecture material. Some of my efforts, as you would observe in this lecture, are products of collaboration among team. Thus, it is important to note that, whenever and wherever I use “we” or “our” in this lecture, I simply imply myself and other team members that have contributed to the work under focus. These include but are not limited to my mentors, co- researchers, teachers, lecturers, students, and colleagues as the case maybe. Therefore, I humbly welcome you on board as we journey on the path to the cloud as we explore the Nigeria digital landscape.

1.0 INTRODUCTION

Mr. Vice Chancellor Sir, the term information technology has in recent times become a popular language across all ages. The educational industries not only use the term but are today completely immersed in the technology in carrying out everyday official tasks. So also do other sectors, such as the business sphere, government, and everyone else. We live in an information age where information emanates from everything we do. Storing and maintaining the information becomes as crucial as the information itself. Computer gadgets and other associated technologies are equally permeating the global space to meet up with the task of information management (Chinedu et al., 2026).

The world has witnessed unprecedented technological transformation over the past few decades. What was once the preserve of large corporations and government agencies has become accessible to individuals, small businesses, and community organizations. This democratization of technology has been driven by several factors: the proliferation of affordable computing devices, the expansion of internet connectivity, and perhaps most significantly, the emergence of cloud computing as a viable alternative to traditional IT infrastructure.

Mr. Vice Chancellor Sir, allow me to take you on a journey. A journey that begins with the humble beginnings of computing, traverses through the evolution of information technology, and arrives at what I believe is the most transformative computing paradigm of our time—the cloud. Along this journey, we shall encounter the fears and hesitations that have slowed cloud adoption in Nigeria, examine the legitimate concerns that underlie these fears, and ultimately discover that the pathway to the cloud, while not without its challenges, is a journey worth taking.

1.1 Computer Science, Information Technology and Information Systems

In a fast-emerging world of Technology, it is not uncommon for individuals to use the terms computer science and information technology interchangeably, simplifying anything related to computers under these broad umbrella terms. While the former delves into theory,

computation and algorithms, the latter focuses on the practical implementation and application of computer systems and networks for business needs. The primary distinction lies in the focus and responsibilities of professionals in each field. Computer Science professionals are primarily involved in developing and enhancing computer programs, leveraging mathematical principles and theories. In contrast, IT professionals are dedicated to the practical aspects of installing, managing and optimizing these programs to fulfill the technological requirements of organizations (UND Blog, 2025).

However, the term technology in Information Technology here refers to the application of tools or equipment for a particular purpose. Therefore, Information technology (IT) is defined as the use of appropriate tools and equipment for the purpose of gathering data, storage data, manipulating data into information and transmitting the information to end users. Two major technologies are useful in information technology. These are (Mell and Grance, 2023; Tanenbaum and Van Steen, 2022):

I. Computer Technology

II. Communication Technology

These technologies aid in the collection of data using suitable input unit/devices, store the data in memory, from where the processing is performed and eventually communicate the resulting information through output unit/devices. The recipient of this information may be stationed at a remote distance. Hence, suitable communication equipment would be required to transmit and deliver the information to end users. This whole process happens when we sit down to prepare a document with any software and sending same over the internet to someone in another location.

An Information system (IS) is a formal, sociotechnical, organizational system designed to collect, process, store, and distribute information. Any specific information system aims to support operations, management and decision-making (Campbell-Kelly et al., 2023; Laudon & Laudon, 2022). Information Systems (IS) are integrated sets of components (hardware, software, data, people, processes) that collect, process, store, and distribute data to support decision-making,

coordination, and control in organizations, transforming raw data into useful information for achieving business goals, like managing operations or interacting with customers. They are fundamental to modern business, powering everything from financial management to e-commerce platforms like Amazon and eBay and involve both technology and the human/organizational context in which it's used.

1.2 The Evolution to Cloud Computing (How Did We Get Here?)

From Mainframe Centralized Compute to Distributed Compute and Back Again!

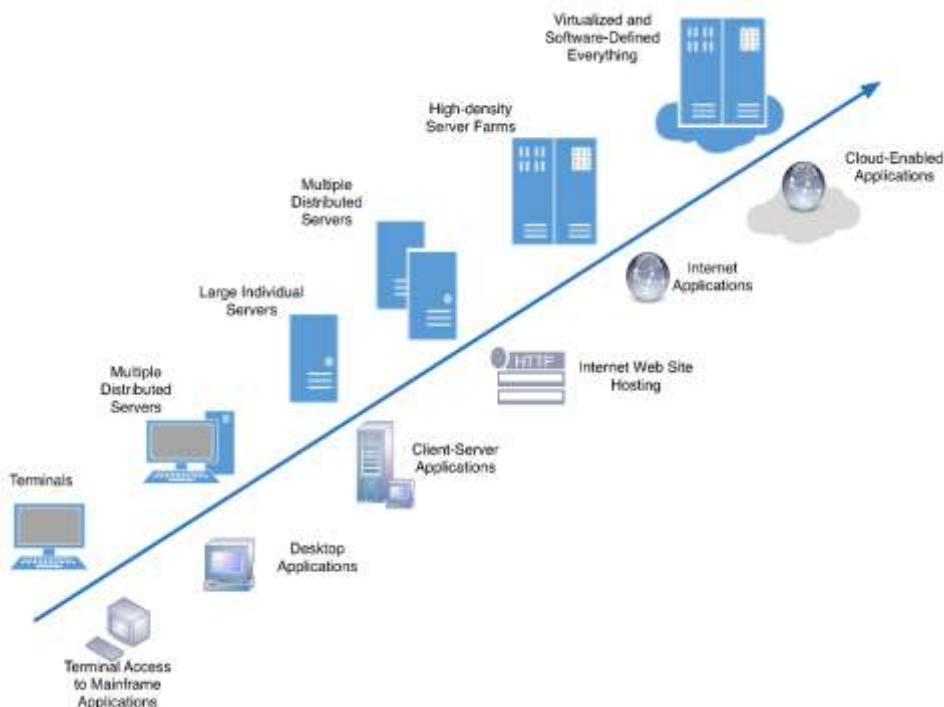


Figure 1: The Evolution to Cloud Computing [Source: Bond, 2015]

[Diagram showing the cyclical evolution from mainframe computing through distributed computing to modern cloud environments]

Mainframe Centralized Compute: In the early days of computer technology, the mainframe computer was a physically very large, centralized computing platform with terminals used by end-users. This centralized mainframe held all the computing power (CPU), memory, and storage systems managed by a small staff for shared use by a massive number of users. There are further similarities when comparing mainframe computing environments to today's cloud (Bond, 2015; Campbell-Kelly et al., 2023; Chinedu et al., 2026).

Distributed Computing: For about 20 years starting in the late 1980's and into the year 2000, the industry began a huge shift to distributed computing with small servers (compute devices). Each server held more memory, CPU, and storage than even the best mainframe, but had inferior levels of shared computing, shared management, and I/O performance (Bond, 2015; Chinedu et al., 2026).

Transforming to Consolidated Computing: Most large organizations have numerous data centers, server farms, storage, and applications spread across offices, campuses, and cities worldwide. Organizations have realized that the cost of these numerous and distributed facilities is too expensive and inefficient for many reasons (available skilled labor, physical location/asset costs, maintenance and upkeep, etc.) (Bond, 2015; Chinedu et al., 2026).

The Evolution to Today's Cloud Environment: In a relatively short period of time, we have gone from centralized compute processing with thin end-user/edge devices (called terminals) to highly distributed compute environments and are now headed back to centralized computing once again (Bond, 2015; Mell & Grance, 2023; Chinedu et al., 2026).

Mr. Vice Chancellor Sir, what makes this observation particularly striking is the cyclical nature of technological evolution. What is old becomes new again, but with significant improvements. Today's centralized cloud environments are not a return to the mainframe era; they represent something fundamentally different—a marriage of centralized management with distributed accessibility, of shared resources with individual customization, of economies of scale with personal empowerment.

1.3 The Pathway to the Cloud

Cloud computing is a major component and application of both **Information Technology (IT)** and the broader field of **Information and Communications Technology (ICT)**. While IT is focused on the use of computers, networks, and software to manage data, ICT encompasses IT and integrates it with telecommunications and other communication tools. The reason these two terms are slowly becoming synonymous is that many modern communications technologies are digital. As more IT technologies begin to include communications, the distinction between IT and ICT will slowly fade. Thus, within this lecture, both terminologies would be used interchangeably to connote the same thing.

1.4 The Metaphor of 'Going Cloudy'

The metaphor of 'going cloudy' in cloud computing refers to shifting from local, owned IT (like on-premises servers) to using remote, internet-based services (the "cloud") for data storage and processing, making services accessible anywhere, anytime, without managing the underlying hardware. While a convenient shorthand, "cloudy" can also imply ambiguity, complexity, or potential issues with access (like a foggy day), highlighting the need to understand security, reliability, and provider differences, as it's just someone else's computers.

1.4.1 Key Aspects of the Metaphor

- a. **Origin in Diagrams:** Tech diagrams used cloud shapes to represent the vast, complex internet infrastructure, hiding the messy details, a practice dating back to the 1990s.
- b. **Abstraction of Complexity:** "Going cloudy" means relying on the internet to access resources (software, storage, servers) that you don't physically own or manage, much like a real cloud hides the sky.
- c. **Accessibility & Flexibility:** It's about renting resources ("pay-as-you-bake" bakery analogy) for scalability and remote access, rather than buying and maintaining your own.
- d. **The "Cloudy" Caveat:** While convenient, the term can be misleading; it's not a magical entity but real servers, and "cloudy" can mean uncertain, complex, or prone to outages if not managed well (like bad weather).

1.4.2 Examples of "Going Cloudy"

- a. Using Gmail or Dropbox (storing files online).
- b. Running a web application hosted on Amazon Web Services (AWS) or Microsoft Azure.
- c. Streaming video from Netflix.

In essence, "going cloudy" means embracing the internet as your computing utility, but with the responsibility of ensuring your cloud strategy is secure and robust, not just a hazy, unpredictable service.

Mr. Vice Chancellor Sir, it is this very haziness that has generated fear among potential cloud adopters in Nigeria. When you cannot see, touch, or physically secure your data, the natural human response is apprehension. But as we shall see throughout this lecture, these fears, while understandable, are often based on misconceptions about what the cloud actually is and how it operates.

1.5 Problem Statement

Globalization and the economic pressures following the COVID-19 pandemic have fundamentally changed customer expectations. Enterprises now demand IT solutions that offer superior availability, scalability, and efficiency. This shift has accelerated the search for

alternatives to traditional on-premises infrastructure. The increasing interest of a broad-based business leaders and organisations centre on how best cloud computing can contain these requirements to reduce or eliminate the huge capital outlay for infrastructure ownership, increase efficiency, ensure higher return on investment (ROI), dynamic provisioning and utility—such as pay-as-use services.

The shift from local on-premises IT Enterprise solution to the virtualized cloud environment by many organisations has been necessitated by the following challenges and requirements within the Nigeria digital landscape:

- i. **Infrastructure Deficiencies:** Unreliable power supply and poor internet connectivity remain significant obstacles. Many organizations cannot maintain the continuous power and bandwidth required for effective on-premises IT operations.
- ii. **Huge Initial Capital Outlay:** The financial constraint of modern IT infrastructure acquisition is particularly acute for small and medium enterprises. The cost of servers, storage systems, networking equipment, and the facilities to house them often exceeds the entire annual budget of many organizations.
- iii. **Huge Maintenance Cost:** Beyond initial acquisition, the ongoing costs of maintenance—hardware replacement, software licensing, staff salaries, cooling, security—continue to drain organizational resources.
- iv. **Focusing on Core Mandates:** Organizations increasingly recognize that IT infrastructure management is not their core business. Maintaining servers and networks distracts from the primary mission of the organization, whether that is banking, education, healthcare, or manufacturing.
- v. **Requirement for Skilled Technical Personnel:** The shortage of qualified IT professionals in Nigeria makes it difficult for organizations to recruit and retain the talent needed to manage complex IT environments.

vi. **Aversion to Change:** Human nature resists change, particularly when it involves perceived loss of control. Many organizations have "always done it this way" and are reluctant to embrace new models.

vii. **Security Concerns:** This is perhaps the most significant barrier. Organizations fear that moving data to the cloud increases vulnerability to attacks, data breaches, and unauthorized access.

viii. **Lack of Visibility and Competitive Advantage:** Organizations without cloud capabilities find themselves at a competitive disadvantage compared to those leveraging cloud flexibility and agility.

However, the slow adoption of cloud computing by many organizations such as those with high business economic drives and those with very sensitive security concerns raises huge concerns. A number of these enterprises within the constituencies of various consumers of cloud services along with some information security professionals have expressed fears on the path to the cloud, stating their unflinching consciousness on security and privacy issues associated with this new computing platform for the next generation of the Internet (Chinedu et al, 2013; Chinedu, 2014).

Mr. Vice Chancellor Sir, let me be clear. These fears are not unfounded. The security of data in the cloud is a genuine concern that deserves serious attention. But the question we must ask is: are these fears proportional to the actual risks? And more importantly, are they preventing us from accessing opportunities that far outweigh the risks? The answer to both questions, as my research demonstrates, is more complex than a simple yes or no.

1.6 Aim and Objectives

This inaugural lecture aims to Introduce the concepts of Cloud Computing as an emerging IT Model, demystify the fears to overcome barriers to Cloud service adoption and deployment by potential cloud subscribers, highlight some of my research efforts related to cloud computing with contribution to knowledge and make some notable recommendations required on the journey to the cloud environment.

The specific objectives of this lecture are to:

- a. Unveil the anatomy of fear in the adoption of cloud environment.
- b. Describe the steps in the cloud computing threat model for a purposeful security solution.
- c. Analyse the cloud security and privacy issues among cloud consumers or the IT professional in the Nigerian constituency.
- d. Re-assess and situate cloud computing security and operational challenges/risks within Nigeria's digital landscape.
- e. Prescribe suitable solutions in a bid to remedy the fears of cloud adoption.
- f. Unveil recent policies, strategies implementations in Nigeria enabling Cloud Computing.

1.7 Scope

In this inaugural lecture, I will cover the following areas:

- a. Introduction of the concepts of Cloud Computing, Demystifying the fears and overcoming barriers to Cloud service adoption and deployment by potential cloud subscribers.
- b. My contributions to Knowledge in the field of Cloud Computing.
- c. My Conclusion and Recommendations.

2.0 UNDERSTANDING CLOUD COMPUTING

Mr. Vice Chancellor Sir, **a cloud is a pool of virtualized computer resources** (Ullah et al. 2018). It is more than a collection of computer resources; hence it provides a mechanism to manage those resources. By means of provisioning, change requests, re-imaging, workload rebalancing, de-provisioning, and monitoring. **Cloud computing** is a term that describes both a platform and type of application. **A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed.** Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices (Roy and Jain, 2015; Chinedu et al, 2020).

Software Testing Help (2021), and Chinedu and Osuagwu (2018) have described **cloud computing as nothing but a way for renting the Software, Platform and/or Infrastructure hosted by a provider**. The word Cloud implies that services provided by the service provide is accessed over the Internet. Thus, it is the cloud service provider that installs, maintains, scales and monitors hardware and/or software services for its customers who access these services via the Internet. Chinedu and Osuagwu (2018) noted that cloud computing also includes applications extended to be provisioned through the Internet. These cloud applications are run in large data centres driven by distributed servers.

2.1 Cloud Computing Service Models

Our understanding and appreciation of cloud computing are better grasped through adequate discussion of the three computing services models that come under its canopy. These models also described as delivery models (Reily et al, 2011) are:

- a. Software as a Service—SaaS—as "Selling ready- to- use application/software"
- b. Platform as a Service—PaaS—as "Access to a configurable platform/API"
- c. Infrastructure as a Service—IaaS—as "Selling virtualized hardware" (Hasan, 2011; Siddiqui, 2011)

The cloud computing stack of Figure 2 shown below would be beneficial in revealing the place of these services.

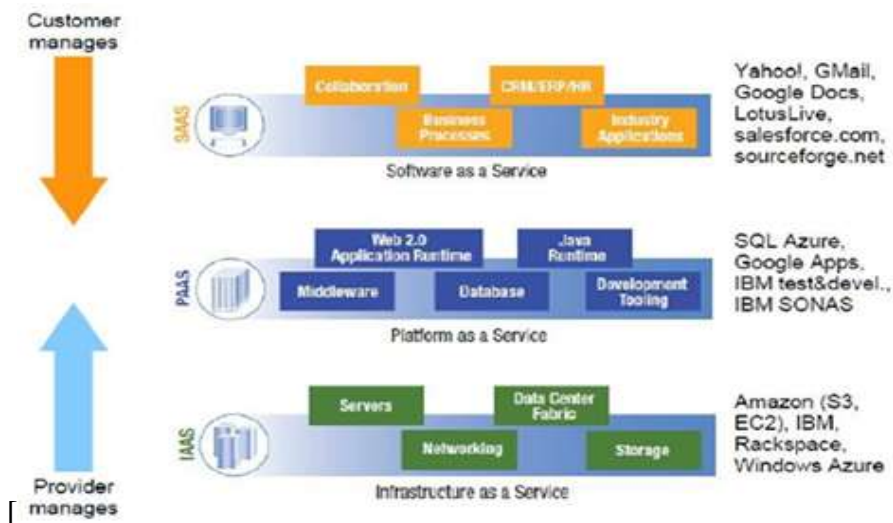


Figure 2: Cloud computing service models showing the three delivery models [Source: IBM Research, 2011]
[Diagram showing the layered architecture of IaaS, PaaS, and SaaS]

The demonstration of adequate understanding of these three delivery models has significantly shed light on creative ways in which a few companies have implemented cloud services at different levels. Obviously, organizations could conveniently go virtual or collaborate in virtual organizing by leveraging on the any or the entire cloud service provision. Thus, rather than concerned itself with the huge initial capital and maintenance cost of owing such cloud services, could allow the cloud service provider to provide the needed intensive ICT resource support to help her concentrate on core business in a virtual environment.

To be considered "cloud", Reily et al (2011) maintained that these delivery models must be deployed on top of cloud infrastructure that satisfies the following **five characteristics**:

1. On-demand self-service
2. Ubiquitous network access

3. Location independent resource pooling
4. Rapid elasticity
5. Pay per use (Reily et al, 2011)

2.2 Cloud Computing Deployment Models

The five deployment models are:

1. **Private (internal) cloud:** enterprise owned or leased, behind a firewall
2. **Public (external) cloud:** sold to the public, mega-scale infrastructure (e.g. Amazon EC2)
3. **Hybrid cloud (virtual private cloud):** composition of two or more clouds (e.g. Amazon VPC)
4. **Community cloud:** shared infrastructure for specific community (e.g. academic clouds)
5. **Multi-Cloud:** utilizes services and resources from several cloud providers, which can be public, private, or hybrid clouds (Reily et al, 2011; Pedamkar, 2023).

The cloud computing deployment Model of Figure 3 shown below helps to elucidate on the degree of cloud resources cloud consumers could deploy at each model.

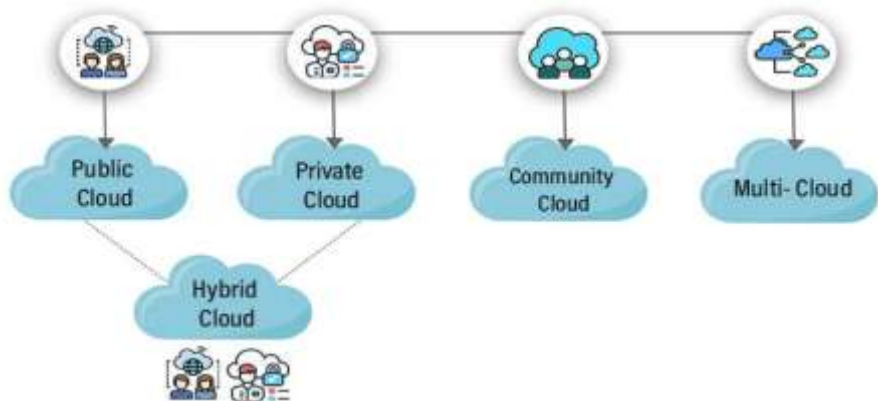


Figure 3: Cloud Deployment Models: Types with Key Factors
[Source: Pedamkar, 2023]

[Diagram comparing public, private, hybrid, community, and multi-cloud deployment models]

Accordingly, anyone who has Internet access or connection could access a cloud application following subscription. However, security pervades technology (Nwankwo, 2020) and by extension the security issues in a cloud computing environment are better grasped through adequate assessment of the risks and threats associated with the three computing models that come under its canopy (Chinedu et al, 2013; Chinedu et al, 2020; Harkut, 2020).

However, with these risks and threats there are numerous benefits (both business and security wise), which form the bedrock for the attractions of most cloud consumers on their journey to the cloud. Chinedu et al. (2013), in a paper titled "Enterprise Cloud Adoption: Leveraging on the Business and Security Benefits" explored extensively on some of these benefits, which has been tabulated in table 1 below:

Table 1: Various Benefits of Cloud Computing

Business Benefits	Security Benefits	Technical Security Benefits
1. Cost Containment 2. Immediacy 3. Availability 4. Scalability 5. Efficiency 6. Resiliency 7. Software as a subscription 8. Reduced Software Maintenance 9. Increased Reliability 10. Environmentally Friendly 11. Stays Current: 12. Versionless Software	1. Reduces the exposure of sensitive data 2. Simplifies security auditing & testing 3. Enables automated security management 4. Improves redundancy & disaster recovery	1. Centralized Data 2. Incident Response / Forensics 3. Password assurance testing (aka cracking) 4. Logging 5. Improve the state of security software (performance) 6. Secure builds 7. Security Testing

2.3 Essential Characteristics of Cloud Computing

As may be observed in the characteristics presented in Table 2, there are many approaches and challenges to cloud computing. The benefits to the enterprise, as well as the risks, will vary depending on the types of service and deployment models subscribed to (ISACA, 2009; Chinedu and Osuagwu 2018; Chinedu et al, 2020).

Table 2. Cloud Computing Essential Characteristics

Characteristic	Definition
On-demand self service	The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service's provider.
Broad network access	According to NIST, the cloud network should be accessible anywhere, by almost any Device (e.g., smart phone, laptop, mobile devices, PDA).
Resource pooling	The provider's computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence. The customer generally has no control or knowledge over the exact location of the provided resources. However, he/she may be able to specify location at a higher level of abstraction (e.g., country, region or data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in many cases automatically, to scale out quickly and rapidly released to scale in quickly. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service (Pay as you go)	Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and customer of the utilized service.
-------------------------------------	---

2.4 The Anatomy of Fear: Understanding Cloud Security Concerns

Historically, enterprises and users feel more comfortable and confident in storing and maintaining their data on their private computers located in their private network environments. The present concern expressed by Siddiqui (2011) with the advent of cloud computing where the data storage would be provided (and controlled) by the provider is that the enterprises and individuals would have to part with their data if they want to enjoy the benefits of the cloud and this is the origin of the concerns for security (Chinedu et al, 2020).

The concern is that total control is maintained where the data infrastructure are housed within the boundaries of the organization and for which appropriate security mechanisms could be implemented. Installations of hardware and trusted software could be done with ease to create secure perimeter around the internal network; 'security-by-complexity' could be affected by adding multiple layers of security, etc. However, once the data leaves the private network into the cloud, the owner loses control over it as well as the security around it. In the cloud, total dependence as to the security of the data is on the provider to offer these services (Siddiqui, 2011).

The fears based on the concern of where the data emanated from (traditional standalone/network environment), and where it is going (cloud computing—"going cloudy") have been examined and hence outlined by Hasan (2011), against the following security, privacy and forensic issues (Chinedu, 2018; Chinedu et al, 2020):

A. Confidentiality

1. Will the sensitive data stored on a cloud remain confidential? Will cloud compromise leak confidential client data (i.e., fear of loss of control over data)?
2. Will the cloud provider be honest and won't peek into the data?

B. Integrity

1. How does the data owner know that the cloud provider is doing the computations correctly?
2. How would the subscriber ensure that the cloud provider really stored his data without tampering with it?

C. Availability

1. Will critical systems fail if the provider is attacked in a Denial of Service attack?
2. What happens if cloud provider goes out of business?

D. Privacy issues raised via massive data mining

1. Cloud stores data from a lot of customers, and can run data mining algorithms to get large amounts of information on clients

E. Increased attack surface

1. The entities outside the organization store and compute data, and so attackers can target the communication link between cloud provider and clients
2. Cloud provider employees could be involved in phishing attacks

F. Auditability and forensics

1. It is difficult to audit data held outside the organization in a cloud
2. Forensics is made difficult since clients don't maintain data locally

G. Legal quagmire and transitive trust issues

1. Who is responsible for complying with regulations?
2. If cloud provider subcontracts to third party clouds, will the data still be secure? (Hasan, 2011; Chinedu, 2018; Chinedu and Osuagwu, 2018; Chinedu et al, 2020)

Mr. Vice Chancellor Sir, these are practical issues that are militating against the adoption of cloud computing. The onus lies with the providers, if they want to win the trust of incredulous potential

customers and gain competitive edge in the marketplace, to speedily address the matters of security first. But let me also make a crucial observation: many of these same fears were expressed when the internet itself was being introduced, when e-commerce was emerging, and when mobile banking was first proposed. In each case, legitimate security concerns were addressed through technological innovation, regulatory frameworks, and the development of industry best practices. The cloud is no different.

2.5 Cloud Computing Threat Model

According to Metri et al. (2011), it is difficult to build a secure platform without taking a major preliminary step such as appreciating and identifying the various threats to the proposed online platform. A threat model is a model which helps in analyzing a security problem, design mitigation strategies, and evaluate solutions (Hasan, 2011; Cho, 2010; Metri et al., 2011; Chinedu and Osuagwu, 2018).

Metri et al. (2011) further described this model as a theorem which incorporates the following steps to reach the solution to the problem:

Step 1: Identify attackers, assets, threats and other components

Step 2: Rank the threats

Step 3: Choose mitigation strategies for the threats

Step 4: Build solutions based on the strategies

Mr. Vice Chancellor Sir, what this threat model demonstrates is that security is not a destination but a journey. It is not something that can be achieved once and forever, but a continuous process of assessment, adaptation, and improvement. The cloud, like any other computing environment, requires this ongoing attention to security.

2.6 Cloud Data Security: Concerns and Solutions

In a survey, IBIS Technology (2020) ranked security as top concern among 81% of business owners, and equally admitted that the cloud is one of the most secure environments to protect data. However, IBM Research (2011), highlights five key concerns about cloud computing. These gave foremost priorities to the issues of **"less control" of user to**

their data, and data security in a shared network and compute infrastructure to unveil threats on and discomfort by many companies and governments with the concept of locating data on systems not user controlled and the **increasingly potential for unauthorized exposure in multi-tenant environment** respectively (Chinedu, 2018; Chinedu and Nwankwo, 2018; Chinedu et al, 2020).

Ghani et al (2020) further argued that with **increase in size of the data**, there is also an increase in data attacks and interceptions in the virtual environment. According to the submission, virtualized environment of cloud computing presents storage services where a user has no control over their data. Under such circumstance, a consumer's concern borders on questions as to: where exactly his data are located, what happens if he deletes his data and whether or not the deleted data were really permanently deleted. These concerns were debunked in a report by IBM Research (2011); Chinedu and Nwankwo (2018). Chinedu and Nwankwo (2018) had proffered the following solutions:

1. **Less control: Provider become fully security transparent and offer sophisticated control**
2. **Data security, wherein the following are implied:**
 - a. Implement secure authentication, authorization, and identity management
 - b. Isolate multiple tenants from each other
 - c. Encrypt critical data and ensure they are integrity-protected by client.

Encryption involves using a cryptographic algorithm and a cryptographic key in order to transform a plaintext into a ciphertext or not obvious text (Al Beshri, 2013). Thus, encryption is an information security measure that renders data unintelligible to unauthorized readers. According to Hellman (1980) "encryption is a coded transformation of data into a form unreadable to intruders and interlopers who lack the appropriate key to decrypt the encoded data." Encryption is gaining popularity as social and community computing (such as the cloud) is gaining momentum.

Data are the most important resource to a user, and in a public cloud where communal computing and multitenancy are practiced, encryption must be inevitable to ensure confidentiality and integrity of data and data bank. Encryption is implemented to curb impersonation, wiretapping, piracy, spoofing and data diddling which are common abuses in a multi-user environment. There are different encryptions algorithms such as Blowfish, Rijndael, AES, Crypt, etc to combat some of the known threats.

Mr. Vice- Chancellor sir, protection of user data against data breaches in cloud applications and the potential security failures of the service providers coupled with heightened cloud user fears or worries on cloud adoption, have in no small degree challenged measures taken to demystify fear to cloud services, so as to unveil its enormous capabilities and awesome benefits such as accessibility, availability, collaboration, to name a few. Obviously, the security of the cloud infrastructure entails protecting cloud data from unauthorized access, preventing malicious programs from corrupting the virtual resource and ensuring the secure cloud data remains unintelligible to any unauthorized access or intrusion by malicious users.

2.7 Nigeria-Specific Risk Analysis of Cloud Deployment and Service Models

Mr. Vice Chancellor Sir, having examined cloud security concerns in general terms in the preceding sections, it is instructive to now situate these concerns squarely within Nigeria's digital landscape. Cloud computing is undeniably driving digital transformation across the country, yet adoption remains slow among institutions, government agencies, and Small and Medium Enterprises (SMEs). The reluctance to "go cloudy" stems from two distinct angles: the deployment model, which concerns where the cloud is hosted, and the service model, which concerns what is being managed by the provider.

2.7.1 Risks Inherent in Cloud Deployment Models

Deployment models define who owns and controls the underlying infrastructure. Table 3 evaluates the risk profile of each model as it applies to the Nigerian context.

Table 3: Risks Inherent in Cloud Deployment Models for Nigeria

Deployment Model	Key Risks for Nigeria	Evaluation / Impact
1. Public Cloud (AWS, Azure, GCP, Oracle)	Data Sovereignty & Jurisdiction — data stored outside Nigeria is subject to foreign laws such as the US CLOUD Act and GDPR. Vendor Lock-in — proprietary APIs make migration difficult. Internet Dependency — Nigeria's bandwidth cost and downtime affect access.	High Risk. Government and MDAs fear sensitive data such as NIN, BVN, and health records leaving the country. SMEs fear sudden price hikes. A majority of Nigerian firms cite internet reliability as a barrier to cloud adoption.
2. Private Cloud (on-premise or hosted for one organisation)	High CAPEX — the cost of servers, power, cooling, and staff is substantial. Skill Gap — few local engineers are able to manage private cloud environments. Scalability Limitation.	Medium Risk. Suited to banks and government agencies handling sensitive data, though power and diesel costs in Nigeria make it expensive. Remains the preferred model for institutions such as the CBN and NIBSS.

3. Hybrid Cloud (mix of public and private)	Complexity — difficult to manage security consistently across two environments. Data Integration Risk — synchronizing on-premise and cloud systems can create data leaks. Cost Overrun.	Medium-High Risk. Regarded as the safest model for Nigerian banks, but it requires strong IT governance, which many organisations lack.
4. Community Cloud (shared by a few organisations, e.g., universities, health sector)	Shared Responsibility Confusion — ambiguity over liability in the event of a breach. Trust Issues — competitors may share the same community cloud.	Low-Medium Risk. Not yet common in Nigeria, though the Nigerian Research and Education Network (NREN) could adopt this model for universities. The principal risk lies in governance.

Mr. Vice Chancellor Sir, the biggest deployment-related fear in Nigeria is the twin concern of data sovereignty and internet reliability. With the Nigeria Data Protection Regulation (NDPR) 2019 and the Nigeria Data Protection Act (NDPA) 2023 now in force, transferring citizen data abroad without adequate safeguards constitutes a legal risk, not merely an operational inconvenience.

2.7.2 Risks Inherent in Cloud Service Models

Service models define the division of responsibility between the subscriber and the provider. Table 4 sets out the corresponding risks for Nigeria.

Table 4: Risks Inherent in Cloud Service Models for Nigeria

Service Model	What Provider Manages	Key Risks for Nigeria	Evaluation / Impact
1. IaaS (e.g., AWS EC2, Azure VM)	Servers, storage, network	Misconfiguration — most breaches originate from open storage buckets or firewalls. Underutilisation — pay-as-you-go billing leads to bill shock in Naira terms due to exchange-rate exposure.	Medium Risk. Offers control but requires skilled DevOps personnel. FX volatility makes dollar-denominated billing a major concern for SMEs.
2. PaaS (e.g., Heroku, Google App Engine)	Operating system, runtime, middleware	Loss of Control — subscribers cannot patch the operating system or tune the database. Vendor Lock-in — code becomes tied to the provider's platform.	High Risk. Nigerian developers fear an inability to exit easily, compounded by limited local PaaS alternatives.
3. SaaS (e.g., Google Workspace, SAP, QuickBooks)	Everything, including the application	Data Breach & Privacy — HR and finance data reside on vendor servers. Service Outage — business operations halt if the SaaS platform is unavailable. Compliance —	Highest Risk. This is the primary source of "going cloudy" apprehension. Government agencies are particularly wary of hosting

		uncertainty over whether the SaaS meets NDPA 2023 requirements.	payroll and student records on foreign SaaS platforms.
4. DaaS / FaaS (Desktop/Function as a Service)	Desktop provisioning, code execution	Security — functions can serve as entry points for attack. Monitoring challenges.	Low-Medium Risk. Still an emerging model within Nigeria.

The biggest service-model fear in Nigeria centres on SaaS and data privacy, since this model hands full custodianship of institutional data to a foreign entity. Amid rising cybercrime, organisations continue to ask: if the provider itself is breached, who bears liability?

2.7.3 Nigeria-Specific Fears Amplifying These Risks

Beyond the deployment and service model dimensions above, several country-specific conditions compound the perceived risk of cloud adoption in Nigeria:

- I. **Regulatory and Legal Risk** — the NDPA 2023 requires data localisation for certain categories of data, yet clear guidance on cross-border transfer remains limited.
- II. **Power and Connectivity Risk** — cloud services are of little value without stable power and internet access; the cost of diesel further raises the price of private cloud deployment.
- III. **Cybersecurity Risk** — Nigeria ranks among the countries most exposed to cybercrime globally, fuelling fears of data theft and ransomware in cloud environments.
- IV. **Cost and Foreign Exchange Risk** — major cloud providers bill in US Dollars, so Naira devaluation can raise the effective cost of cloud services substantially each year.

- V. **Skills Gap Risk** — a small minority of IT staff hold recognised cloud certifications, generating concern that adopting institutions "won't be able to manage it."
- VI. **Vendor Lock-in and Exit Risk** — organisations worry about how they would retrieve their data should a provider raise prices or withdraw from the Nigerian market.
- VII. **Trust Deficit** — following a number of fintech data breaches, public institutions remain reluctant to entrust sensitive data to third parties.

Mr. Vice Chancellor Sir, the riskiest combination is Public Cloud paired with SaaS for sensitive government data, while the safest pathway for Nigeria going forward is a Hybrid Cloud approach combined with IaaS or PaaS delivered through local providers, supported by deliberate skills-building and regulatory enforcement.

3.0 RESEARCH METHODOLOGY

3.1 Research Approach and Design

Mr. Vice Chancellor Sir, this research adopted a quantitative approach which involves quantity and measurement as well as interaction with stakeholders. The quantitative approach was chosen because it allows for the systematic collection and analysis of numerical data that can be generalized to the broader population of cloud computing stakeholders in Nigeria. This approach is particularly suited to the study of technology adoption, where measurable patterns and relationships can be identified.

The research design combined descriptive and analytical elements. Descriptive elements captured the current state of cloud computing awareness, adoption, and concerns among Nigerian organizations. Analytical elements examined the relationships between variables such as organization type, security concerns, and adoption decisions.

3.2 Population and Sampling

Data were collected from a sample population including technology experts and professionals from the financial and services industry

(Chinedu, 2018; Chinedu and Nwankwo, 2018). The financial and services industry included the banking and insurance companies. This industry subsector was selected through purposive sampling owing to its service delivery architecture, current prospects locally, contribution to the socioeconomic ecosystem as well as their dependence on information technologies.

The technology experts were drawn from the local IT regulatory body—the Computer Professionals Registration Council of Nigeria (CPN) and the college of fellows of the Nigeria Computer Society (NCS). The random sampling technique was employed. The total population sampled was 180 respondents. 124 persons were selected. The 124 persons were considered a fair representation of the stakeholders.

3.3 Data Collection Instruments

A structured questionnaire was constructed and distributed to the 124 respondents, whereas 24 persons from the financial services subsector were interviewed with respect to their information technology business strategy particularly the use of cloud services. The questionnaire was structured to reflect the qualification and experience of the respondents, cloud services benefits to the organization, risks, threats, security concerns and fears in respect of cloud adoption strategy in their respective organizations (Chinedu, 2018; Chinedu and Nwankwo, 2018).

The interviews provided qualitative depth that complemented the quantitative breadth of the questionnaire. They allowed for exploration of nuanced perspectives on cloud computing that might not be captured through closed-ended questions.

3.4 Data Analysis Techniques

Statistical data were captured and sorted using MySQL database and later analysed with SPSS software. The frequency distribution and percentage methods were used to analyze the data. This was adopted based on the wide agreement that the percentage method is useful and

could be validly used for studies including management, scientific and sociological researches (Ike, 2003; Saunders et al, 2007).

4.0 FINDINGS AND DISCUSSION

4.1 Business and Security Benefits of Cloud Computing

Mr. Vice Chancellor Sir, when asked about the benefits they experience or expect from cloud computing, the responses revealed interesting patterns. More flexibility, cost savings, and better scalability ranks high on benefits experiencing from cloud computing.

Majority of the participants indicate that three core drivers of cloud computing are relevant: more flexibility (90 percent), cost savings (72 percent) and scalability of their IT infrastructure (62 percent) (see Figure 4) (Chinedu, 2018; Chinedu and Nwankwo, 2018).

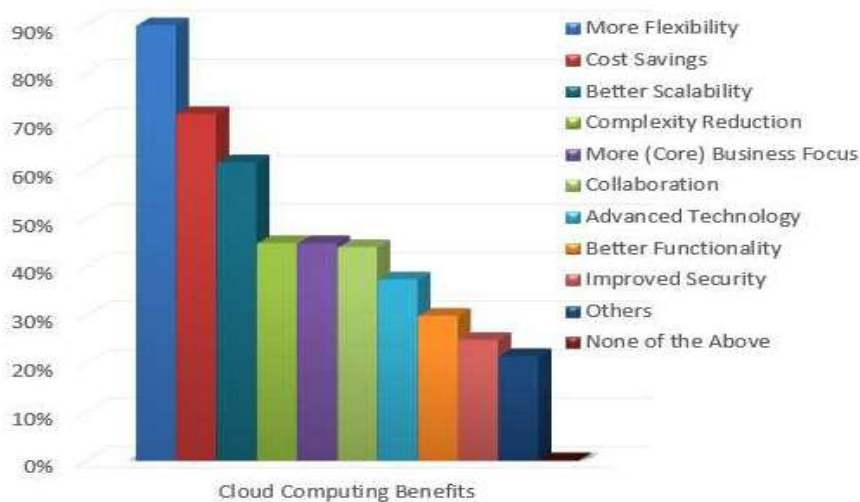


Figure 4: Percentage on business and security benefits.

[Bar chart showing: Flexibility (90%), Cost Savings (72%), Scalability (62%), Improved Security (25%)]

What is particularly noteworthy about these findings is the relatively low percentage (25%) who identified improved security as a benefit. This suggests that while organizations recognize the operational and financial

advantages of cloud computing, they remain unconvinced about its security benefits. This perception gap between perceived and actual security is something that cloud service providers must address through transparency and demonstrable security practices.

4.2 Security and Privacy: The Main Obstacles

Mr. Vice Chancellor Sir, when participants were asked about their main concerns regarding cloud computing, the responses confirmed that security remains the dominant barrier to adoption. In an interview, an overwhelming majority of the participants (71 percent) consider security issues to be their main concern regarding the use of cloud computing. Privacy issues (60 percent) ranked second. Others such as legal (50 percent), and compliance issues (50 percent) are highlighted to be areas of risk or concerns, and blocking issue when it comes to decision on migrating to the cloud (Chinedu, 2018; Chinedu et al, 2020).

Focusing on the security in place with the organisations, 83 percent of participants agree that security solutions are deployed for organisational data. It appears that potential cloud subscribers are not worried primarily about the lack of security measures, but about the lack of transparency on the side of cloud vendors. This is owing to the fact that only 25 percent of these participants indicated that improved security is one of the benefits they experience with cloud computing under our questionnaire (refer to Figure 4).

In an interview, it was argued that though cloud computing no doubt provided a centralized framework where security measures could be optimized, yet most users require sufficient trust on the providers to be able to outsource control of their valuable data to the third party. Thus, it would be deduced that where the threats to user data are mitigated with external parties' intruders or hackers, such data remains more than 70 percent vulnerable to internal threats or attackers from within the third-party cloud provider's premises.

Mr. Vice Chancellor Sir, this finding is particularly significant. It suggests that the fear of cloud computing is not primarily about external hackers or cybercriminals—though those are real concerns—but about

the internal threat posed by the cloud service provider's own employees and systems. When you cannot see who has access to your data, when you cannot audit the security practices of the provider, the natural human response is anxiety. This is why transparency is not just a nice-to-have feature of cloud services but an absolute necessity for building trust.

4.3 Mission-Critical Processes and Sensitive Data

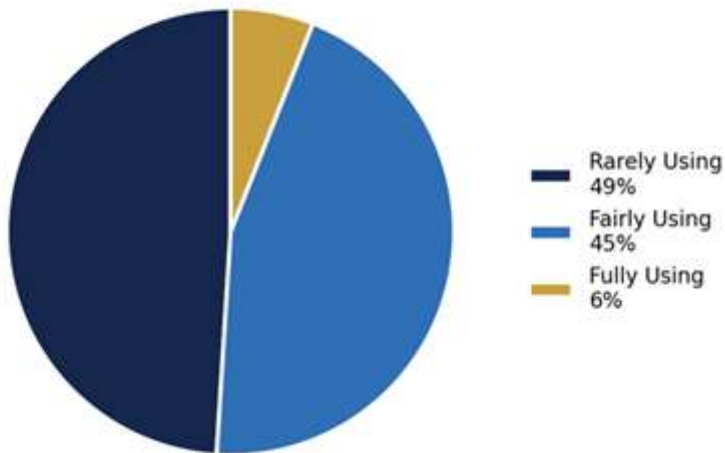


Figure 5: Degree of Deployment/ Movement to the cloud.
[Pie chart showing: Rarely using (49%), Fairly using (45%), Fully using (6%)]

The survey reveals that an average of **49 percent** are **rarely using** or planning to use cloud computing storage services for managing their business-critical processes and extremely sensitive data storage. **45 percent** **fairly use** or plan to use this computing paradigm for same purposes. While only a small fraction representing **6 percent** are **fully using** the cloud computing for their mission-critical applications (See Figure 5).

Mr. Vice Chancellor Sir, this distribution reveals a pattern of cautious exploration rather than enthusiastic adoption. Organizations are willing to experiment with cloud computing for non-critical functions, but when

it comes to their most valuable data and most essential processes, they hold back. This is rational behavior. No organization would entrust its crown jewels to an unproven system. But it also means that organizations are missing out on the full benefits of cloud computing by limiting their adoption to peripheral functions.

4.4 Current Security Solution Implementation

Greater concerns on organisational deployment of user secure authentication with identity management, and securely encrypted with integrity-protected user data have been made by some identified sectors, especially on the part of those of finance and banking businesses. This is evident from the responses of 40 percent of the respondents which indicated that they are to a low degree (virtually not), and the rest (60 percent) participants which indicated they are medium (fairly) considering/implementing these security solution. This aligns with a statement credited to a sales officer at Standard Chartered Bank which is captured thus:

"We are not actually certain how secure the cloud is at the moment, but so far, we can count on the availability as against those previously used on-premise business critical applications. We are said to be on business because of our cloud readiness." — Sales Officer of Standard Chartered Bank—a firm in the financial services sector (Chinedu, 2018).

None (0 percent) of the respondents showed affinity to high degree deployment of user secure authentication with identity management, and securely encrypted with integrity-protected user data as against those of the other businesses such as Education, Manufacturing, Service, and Development (Chinedu, 2018; Chinedu et al, 2020) (see Figure 6).

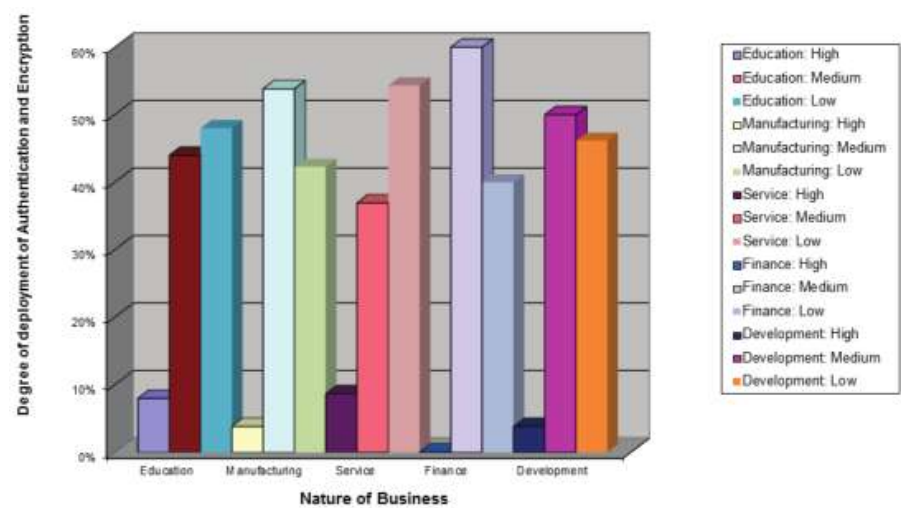


Figure 6: Measures of security solution/ technique.
[Chart showing: Low (40%), Medium (60%), High (0%)]

4.5 Demystifying the Fears: Overcoming Barriers to Adoption

Cloud data security is widely seen as the main barrier to cloud computing adoption, followed by concerns about privacy, compliance, and legal issues. Organisations are particularly worried about external data storage, given risks such as data breaches, data loss, service hijacking, insider threats, and outages (Ardagna et al., 2015). Many potential users feel that cloud service providers (CSPs) cannot fully guarantee absolute data protection, transparency, trust or alignment with internal security requirements. Recurring security incidents have further reduced enthusiasm, especially among organisations handling highly sensitive or mission-critical data (Chinedu, 2018; Chinedu et al., 2020). Despite these concerns, cloud adoption remains attractive due to its economic and operational benefits, including reduced infrastructure costs, long-term IT savings, and pay-per-use models. Avoiding cloud adoption may even put organisations at a competitive disadvantage by increasing costs (Chinedu et al., 2015). However, cloud computing may not suit every organisation. Those with highly classified operations may prefer private clouds despite higher costs. For small and medium-sized

enterprises, private clouds may not be financially viable, making hybrid or virtual private cloud models more practical. These models offer greater control over data access and storage, potentially addressing some security concerns and encouraging hybrid cloud adoption (Chinedu, 2018; Chinedu et al., 2020).

Ultimately, cloud security challenges also present opportunities. CSPs can develop stronger security solutions to build trust and gain competitive advantage, particularly in markets such as Nigeria and globally. As cloud security evolves alongside IT advancements, organisations that adopt cloud computing responsibly can remain competitive without excessive fear of security risks (Chinedu, 2018; Chinedu et al., 2018; Chinedu et al., 2020).

Mr. Vice Chancellor Sir, let me offer a perspective that may help demystify these fears. When you store data in the cloud, you are not storing it in some ghostly, uncontrollable space. You are storing it in a data center—a physical facility that, in many cases, is more secure than your own server room. These facilities have biometric access controls, 24/7 security personnel, redundant power supplies, advanced fire suppression systems, and multiple layers of physical and logical security. The question is not whether the cloud can be secure, but whether you have chosen a provider that takes security seriously and whether you are implementing appropriate security measures yourself.

4.6 Nigeria's Policy Framework for Cloud Computing

Mr. Vice Chancellor Sir, Nigeria's legislative and policy framework has significantly evolved to advance digital transformation, particularly in cloud computing, data protection, and ICT development. The National Information Technology Development Agency (NITDA) plays a central role in driving this transformation through regulatory frameworks, strategic collaborations, and cloud-oriented initiatives. A key instrument is the Nigeria Cloud Computing Policy, which promotes a cloud-first strategy aimed at reducing IT costs, improving efficiency, and enabling scalable digital services across sectors (Chinedu, Nwankwo & Isong, 2021; Chinedu et al., 2025b).

I. National Data Classification and Sovereignty Framework (2025)

To enhance cloud governance and data sovereignty, Nigeria introduced a national data classification and sovereignty framework in 2025 under NITDA's leadership. This framework identifies categories of data that must be hosted within Nigeria to protect sensitive information and maintain sovereign control over critical digital assets. It also supports broader efforts to attract global hyperscale providers, including Google Cloud, to establish local operations and strengthen domestic cloud infrastructure (Chinedu & Hussaini, 2018; Chinedu et al., 2025b).

II. Nigeria Data Protection Act (NDPA) 2023

In 2023, Nigeria enacted the Nigeria Data Protection Act (NDPA), which strengthens personal data protection, imposes stricter compliance obligations, and aligns Nigeria with international data governance standards. Combined with data localization initiatives, the Act enhances investor confidence and reinforces secure cloud adoption (Onatuyeh et al., 2025). Public-private partnerships further operationalize digital transformation. Collaborations between NITDA and global technology firms such as Microsoft aim to implement the Cloud First Strategy across Ministries, Departments, and Agencies (MDAs). These partnerships build cybersecurity capacity, promote innovation, and strengthen digital skills within the public sector (Chinedu et al., 2020; Chinedu et al., 2025b).

III. Nigeria Startup Act and Regulatory Coordination

Beyond specific laws, Nigeria has adopted integrated policy coordination to sustain innovation. The Nigeria Startup Act provides structured support for tech entrepreneurs, while NITDA's regulatory intelligence approach encourages adaptive, innovation-friendly governance. Together, these frameworks foster an enabling ecosystem for cloud computing, artificial intelligence, blockchain, and other emerging technologies (NITDA official release, 2025). Infrastructure development complements these reforms. Investments such as MTN's Tier III data center in Lagos expand

local hosting capacity, reduce latency, and support compliance with data localization requirements—thereby strengthening Nigeria's digital sovereignty (Chinedu, Nwankwo, & Isong, 2021; Chinedu et al., 2025b).

Although challenges persist—including digital skill gaps, infrastructural limitations, and regulatory inconsistencies—the alignment of cloud policies, data protection laws, strategic partnerships, and infrastructure investment demonstrates a coordinated national effort to position Nigeria as a competitive digital economy capable of sustainable socio-economic growth and global integration.

Mr. Vice Chancellor Sir, I am particularly encouraged by these developments. When I began my research on cloud computing over a decade ago, Nigeria had no coherent policy framework for cloud adoption. Today, we have legislation, regulatory frameworks, and strategic initiatives that demonstrate a serious commitment to digital transformation. This is progress. However, policy implementation remains a challenge, and we must ensure that these frameworks are not just documents but are actively enforced and operationalized.

4.7 Cloud Computing's Impact on Nigeria's Economy

Cloud computing has become a foundational digital infrastructure driving economic transformation and productivity in Nigeria. Its growing adoption reflects the country's transition toward a digital economy marked by data-driven governance, fintech innovation, e-commerce expansion, and ICT-enabled public service delivery. Supported by government digital initiatives and private sector investments in data centers and cloud services, cloud computing is increasingly positioned as a strategic enabler of national competitiveness and development (Chinedu, Okeke & Onyeukwu, 2018; Chinedu et al., 2025b).

Economic analyses demonstrate that cloud adoption has made measurable contributions to Nigeria's GDP through enterprise digitization, productivity gains, and innovation spillovers. In 2021,

cloud computing accounted for approximately 0.02% of regional GDP, with projections estimating up to ₦30.2 trillion in cumulative GDP growth by 2033 if adoption accelerates. These figures underscore cloud technology's long-term economic potential (Chinedu et al., 2021; Chinedu et al., 2025b).

Beyond GDP growth, cloud computing promotes broader socioeconomic development by fostering entrepreneurship, job creation, and industrial modernization. By offering scalable, cost-effective access to advanced technologies, cloud platforms empower SMEs to innovate and compete. Key sectors—including banking, oil and gas, and digital entrepreneurship—are leveraging cloud solutions to enhance operational efficiency, profitability, and market expansion. However, limited ICT literacy, infrastructure gaps, and technical skill shortages continue to restrict inclusive adoption (Chinedu et al., 2013; Chinedu et al., 2025b).

Cloud computing also strengthens public sector modernization. Government institutions increasingly rely on cloud infrastructure for digital identity systems, e-governance platforms, healthcare information systems, and educational technologies. The Nigeria Cloud Computing Policy highlights the strategic goal of expanding cloud adoption across public and private institutions to improve transparency, accountability, and economic diversification (Onatuyeh et al., 2025; Chinedu et al., 2025b).

In the financial and commercial sectors, cloud integration enhances digital resilience. Fintech companies, e-commerce platforms, and digital service providers depend on cloud technologies for secure transaction processing, data management, and scalable operations. Evidence indicates that cloud adoption increases productivity, reduces transaction costs, and supports financial inclusion, thereby reinforcing macroeconomic stability (Chinedu et al., 2020; Chinedu et al., 2025b). Despite its transformative promise, cloud computing in Nigeria faces institutional and structural constraints, including inadequate infrastructure, unreliable power supply, cybersecurity risks, regulatory ambiguities, and data sovereignty concerns. These challenges weaken

investor confidence and limit the sector's growth potential. Addressing them requires coordinated policy reform, infrastructure investment, digital skills development, and strengthened cybersecurity governance (Chinedu et al., 2025b).

Overall, examining the economic and social impact of cloud computing in Nigeria is essential. A comprehensive understanding of its GDP contributions, sectoral effects, and adoption barriers will support evidence-based policymaking and align with Nigeria's broader strategy of digital transformation and economic diversification. Cloud computing thus stands as a strategic instrument for sustainable economic growth and long-term socioeconomic advancement (Chinedu, Yakubu & Osuagwu, 2018; Chinedu et al., 2025b).

5.0 MY CONTRIBUTIONS TO THE FIELD OF CLOUD COMPUTING

My Vice Chancellor sir, having journeyed with me on "Information Technology, the pathway to the cloud: Demystifying the fear to 'going cloudy' within the Nigeria Digital Landscape", it would be a pleasure to outline a few of my humble contributions within this focus area in the last sixteen (16) years of teaching, mentoring and research. Special highlights would be made on Three (3) of these publications. This is just a few representations of the focus twenty-two (22) out of over Seventy (70) scholarly publications to my credits. These contributions interwoven within IT, IS and Computer Engineering spans specializations such as Data Communications, Computer Networks, IoT, e-Governance, Cybersecurity, Cloud Computing, and Virtual Organisation Technologies.

5.1 Security of Cloud Virtualized Resource on a SaaS Encryption Solution (2018)

This paper is aimed at building a cryptographically secure cloud application environment. Its major objective is to design and implement an encryption system for protecting valuable data (such as passwords,

messages, files) in the cloud environment. The design and implementation extended some basic security and privacy requirements including data confidentiality, integrity, and availability by considering fairness as a viable factor.

This paper employed the Structured Systems Analysis and Design Methodology (SSADM) in the software development life. It evolves a novel cryptographically-secure cloud algorithm based on a proposed "Deciv Algorithm" tagged "D65-Enc" algorithm that would effectively hide meaningful user data from all external parties to a virtual network as well as the service provider by putting control in the hands of users. The algorithm is carefully crafted to frustrate any cryptanalyst, hacker or cybercriminal who would try to decipher the algorithm. This implementation is expected to assist cloud users in maintaining control over their data whether at rest or in transit within the cloud networks rather than outsource control to external vendors as usual. Moreover this algorithm also improves the existing state of data privacy and security in the cloud.

Mr. Vice Chancellor Sir, the significance of this contribution lies in its recognition that the fundamental problem of cloud security is one of trust and control. When you encrypt your data before it leaves your premises, you maintain control over who can access it—even if the cloud provider's systems are compromised. This is the principle of "encrypt before you send," and it is one of the most effective ways to address the fear of losing control over data in the cloud.

5.2 Optimizing a Cloud Model for Effective and Efficient Collaboration in a Virtual World (2018)

This research developed a novel hybrid cloud-based framework (tagged: Cloud VO) that integrates existing cloud computing service model (IBM Research, 2011) as well as appreciation of Cretus (2012) Cloud VO

concept, with the virtual value creation (VVC) Framework of Virtual Organisation (VO) (Hales, 2005) for effective and efficient collaboration to ensure corporate visibility and competitiveness in the virtual environment. Further, a hypothetic deductive methodology (quantitative approach) involving survey approach was advanced to meet the establish objectives, as well as derive a mathematical model for effective and efficient VO operations within the proposed cloud-based framework.

This resultant model was represented by applying the multiple regression (MR) equation. Therefore, the resultant model based on the VO activities from the MR analysis of the test of the hypothesis (The degrees of virtualization and the successful collaboration do not significantly impact the adoption of the Cloud model of VO.) is given by:

Cloud VO = f (VZ, CB)

Cloud VO = $0.383 - 0.454VZ + 1.438CB$

Where:

Cloud VO = Cloud model of virtual organization = VVC VO = Index of Virtual Value Creation model of Virtual Organisation (Represents the Existing model of Virtual Organisation in the Cloud

VZ = The degrees of virtualization of the Cloud model of VO

CB = The successful collaboration in the Cloud model of VO.

VZ = Degree of Virtualisation (Represents Digitisation, Infrastructure, and ICT Environment i.e. the Foundational Value Driver, Hales, 2005)

CB = Successful Collaboration (Represents index of IS/ IT Strategy for Collaboration. This includes Involvement in collaborative venture, Contributing Core Competences, Benefiting from integrated value Net, and Impact on Corporate Value/Image i.e the functional values driver- Hales, 2005)

Mr. Vice Chancellor Sir, this contribution addresses the organizational dimension of cloud adoption. It recognizes that cloud computing is not just about technology but about how organizations work together in virtual environments. The model provides a quantitative framework for understanding the factors that contribute to successful virtual collaboration. The model, if deployed would create corporate value or enhance corporate visibility and competitiveness in the global digitized business environment. It will further ensure customer satisfaction, shareholder wealth creation and overall stakeholder value creation through optimized collaborative virtual world.

5.3 Secured Cloud-Based Framework for ICT Intensive Virtual Organisation (2018)

Further challenges which emanated in the field work of the said research which were analysed and factored in as essential variable to a proposed mathematical model for a secured cloud-based VO framework in the research concurred with the highpoints of the top concerns about cloud computing in IBM Research (2011). This research addressed these concerns by proffering some encryption measure towards ensuring the security of user data at rest or in transit within the cloud network, which promises to put control in the hand of the user by deceiving any cryptanalyst, hacker or cyber criminals in an attempt to decipher the algorithm producing it.

Applying the general multiple regression (MR) equation ($Y = b_0 + b_1X_1 + b_2X_2 + b_3X_3 + \dots + b_kX_k + c$), we specify appropriate multiple regression model for the proposed new system as follows:

Secured Cloud VO = f (VVC VO, Cloud Sec, Collab. Benefits) (1)

Where:

Secured Cloud VO = Secured Cloud-based Virtual Organisation Model

Cloud Sec = Index of Cloud Security (Represents security solutions of the cloud computing)

Collab. Benefits = Index of Benefits from the Cloud Collaboration (Represents Benefitting from the Cloud Computing Collaboration)

VVC VO = Index of Virtual Value Creation model of Virtual Organisation (Represents the Existing model of Virtual Organisation)

Applying the general multiple regression (MR) equation on the Cloud Collaboration Benefits, we have:

$$\text{Cloud Benefits} = 0.016 + 0.162\text{MF} + 0.120\text{CS} - 0.033\text{BS} + 0.129\text{CR} + 0.143\text{MBF} + 0.315\text{AT} + 0.099\text{BF} + 0.088\text{IS}$$

The resultant model applies the multiple regression equation 1 above. Therefore, the resultant model based on Secured Cloud-Based Virtual Organisation is given by:

$$\text{Secured Cloud VO} = 3.77 - 0.454\text{VZ} + 1.438\text{CB} - 0.296\text{AUTH} - 0.359\text{ENC} + 0.162\text{MF} + 0.120\text{CS} - 0.033\text{BS} + 0.129\text{CR} + 0.143\text{MBF} + 0.315\text{AT} + 0.099\text{BF} + 0.088\text{IS}$$

Where:

AUTH = Authentication

ENC = Encryption

MF = More Flexibility

CS = Cost Saving

BS = Better Scalability

CR = Complexity Reduction

MBF = More Business Focus

AT = Advance Technology

BF = Better Functionality

IS = Improved Security

Mr. Vice Chancellor Sir, this integrated model incorporates multiple dimensions of cloud security—authentication, encryption, multifactor

authentication, and other factors—into a comprehensive framework. It recognizes that security is not a single measure but a system of interlocking controls that must work together to provide effective protection.

Mr. Vice Chancellor Sir, for any organisation wishing to "go cloudy", the pathway to the cloud requires following the suggestion in this lecture which is a pointer towards progression in a new direction. This appreciates that any new technological development may at first elicit fears among stakeholders. History has always had it that while change is permanent embracing the change may have some obstacles in its path. Such adjustments were once recorded against the Internet and e-commerce by financial institutions and their consumers, though those concerns still remain valid, technological advances in the domain of security has helped in reducing their extents.

6.0 CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

Mr. Vice Chancellor sir, Cloud Computing is no longer becoming a hype that will subside but like the Internet and the E-commerce emergence, which originally faced public fear of adoption due to enormous security and privacy concerns, it is now the future model of IT. Leveraging on the attractions to the several economic and security benefits of cloud computing, it is evident that like other technologies which need time to evolve into maturity, the problems of cloud service/delivery would be reduced and gradually disappears following the ongoing immersion by the emerging IT trends (edge computing, serverless computing, quantum computing, AI, AR/VR, IoT, 5G/6G, blockchain, Big data analytic, etc) riding on this new computing paradigm, representing the future IT Model. Better still, these fears are vanishing through the development and adoption of advanced strategies and policy frameworks that are mutually beneficial to all stakeholders.

Thus, it is submitted that with the demonstration of such strategies by both foreign and local CSPs; inclusive of the recent Nigeria government's policies, strategies and initiatives in the area of cloud

computing and digital transformation, organisations and government institutions are generally on the demystified pathway to the cloud. Further, It is my humble submission that cloud users wishing to demystify the fear to 'going cloudy' may leverage the submissions made in this lecture to debunking the Cloud Security challenges, and recent policies, strategies and implementations in Nigeria enabling cloud computing, data privacy and digital transformation. Finally, it would be appropriate to add that the developments in the area of cloud security in this journey leaves us with no option than accept 'going cloudy'.

Mr. Vice Chancellor Sir, let me conclude with a reflection. When I began my academic journey in this field, cloud computing was a nascent concept, viewed with skepticism by many. Today, it is a mainstream technology, essential to the functioning of businesses, governments, and individuals around the world. The journey has not been without challenges, and the fears that I have discussed today are real and legitimate. But they are not insurmountable. With the right policies, the right technologies, and the right mindset, Nigeria can embrace cloud computing and reap its enormous benefits.

The question is not whether we should go cloudy. The question is how we go cloudy—thoughtfully, securely, and strategically. I believe we are on the right path, and I am optimistic about Nigeria's digital future.

6.2 Recommendations

Upon the bedrocks propounded to promote activities in the cloud-based virtualised environment, Chinedu et al (2018b), Chinedu et al (2025b) and Chinedu et al. (2026) seek to proffer the following recommendations which implementation would greatly ameliorate the existing barriers to effective deployment and adoption of cloud computing in Nigeria as a future IT model among the constituencies of the various consumers (individuals, organisations and MDAs) of the services:

a. Infrastructure Development across Urban and Rural Areas

Government must prioritize investments in reliable power supply and high-speed internet connectivity across Nigeria, not just in

major cities. The digital divide between urban and rural areas must be bridged to ensure inclusive cloud adoption.

b. Consistent Implementation and Enforcement of Policies

Policies such as the Nigeria Data Protection Act and the Cloud Computing Policy must be consistently enforced. Organizations must be held accountable for compliance, and there should be clear consequences for violations.

c. Digital and Cloud-Related Skills Through Collaboration

Government, educational institutions, and industry must collaborate to develop training programs that build cloud computing skills. This includes curriculum development in universities, professional certification programs, and continuous professional development for IT practitioners.

d. MDAs to Adopt Cloud-First Strategies

Ministries, Departments, and Agencies should be required to consider cloud solutions as the default option for new IT projects, with on-premises solutions only approved when there is a clear justification.

e. Incentives, Subsidies, and Technical Support to SMEs

Small and Medium Enterprises should receive incentives—such as tax breaks, subsidies, or reduced cloud service rates—to encourage cloud adoption. Technical support programs should also be established to help SMEs navigate the transition.

f. Regulation for Robust Cybersecurity Measures

Cloud service providers should be required to meet minimum cybersecurity standards, undergo regular security audits, and provide transparency reports to their customers. Stricter enforcement of data protection regulations is also essential.

g. Strategic Collaboration between Government and CSPs

Government should partner with cloud service providers to develop localized cloud solutions that meet Nigerian needs and comply with local regulations. This includes encouraging the establishment of local data centers.

h. Nationwide Sensitization and Stakeholder Engagement

Awareness campaigns should be conducted to educate organizations and individuals about the benefits and risks of cloud computing. Stakeholder forums should be organized to gather input from various sectors on cloud-related policies.

i. Proper ICT Funding and Budgetary Allocation

Government and organizations should allocate adequate budgets for ICT infrastructure and cloud adoption. This includes funding for skills development, infrastructure, and security measures.

j. National Project and Programme/Multinational Project

Nigeria should explore participation in multinational cloud-related projects to learn from international best practices and benefit from economies of scale. National cloud initiatives should also be launched to drive adoption in key sectors.

7.0 ACKNOWLEDGMENTS

Mr. Vice Chancellor Sir, at this juncture, I need to appreciate & acknowledge a number of personalities for the various roles they have all played towards both my life and career progression. Firstly, I owe a debt of gratitude to the Almighty God for His loving kindness and benevolence to me and for seeing me through from the very beginning up to this present stage of my life and career. I want to sincerely say **THANK YOU LORD JESUS!**

Vice Chancellor and University Leadership

Immense thanks to our amiable Vice Chancellor - Professor Sunny Awhefeada for his magnanimity and encouragement. Thank you so much sir for providing the enabling environment and much support to package this Inaugural Lecture. The supports and inspiration of other Principal Officers, and members of the University Management, Prof. Presly Obukoadata (Deputy Vice Chancellor), Prof. Akpovughaye Taiga (Provost, Orerokpe Campus), Mrs. Ejiroghene Etobro (Registrar), Dr. Sylvester K. Okoh (Busar) and Prof. Ogochukwu T. Emiri (University Liberian) are worthy of commendation. Special thanks to the Registrar, Mrs. Ejiroghene Etobro for your motherly role to ensure this day come to reality. The Deans of Faculties and of Student Affairs, Heads of Departments, Staff and Students of Southern Delta University, Ozoro, Nigeria are worthy of commendation for all their support all along.

Academic Mentors and Pioneers

My special thanks to heroes and fathers of this noble profession, in particular, Late Professor Oliver Eberechi Osuagwu, Professors Charles Onuwa Uwadia (my PhD external Examiner, a fellow of the Nigeria Computer Society, the President of the Nigeria Computer Society from 2007 to 2011, and President and Chairman-in-Council of the Computer Professionals Registration Council of Nigeria (CPN) from 2017 to 2019), Professor Moses Okechukwu Onyesolu, Professor Godwin E. Nworuh, Prof. (Mrs.) Udoka Felisita Eze, Professor Samuel Mbadike

Nzotta, Dr. Ow Tuck Joon, Dr Rod Allan A. De Lara, and Prof Subrahmanyam Kodukula, Prof. Sellappen, and Prof. Daniel Wong.

Research Collaborators and Colleagues

Some friends and colleagues have remained special in my academic and professional life due to their continuous support and collaboration in some research or academic undertaking through my journey. The following are worthy of my much appreciation and mention: Professor Arnold Ojugo, Professor Wilson Nwankwo, Professor Charles Oluwaseun Adetunji, Prof. Akinola Samson Olayinka, Professor Kingsley Chiwuike Ukaoha, Engr. Dr. Aliu Daniel, Engr. Dr. Braimoh Abdullahi Ikharo, Engr. Dr. Emeka Obasi, Engr. Dr. Kenneth Adama, Dr. Charles Ikeriowu, Mr. Kayode Benson, Momoh Omuya Muyideen, Dr. Kenneth Chukwudi Njoku, Mr. Chidiebere Ugwuiegbulam, and Mr. Chinaka Akagha, Dr. Bofy I. Idiodi, and Mr. Rufus Udochukwu.

Spiritual Support

Special thanks go to my pastors, Group Pastors and Leaders for their spiritual support. Among them include: Group Pastor & Dcns. Christain Nbok, Zonal Pastor Amaechi Udeaku, Zonal Pastor John Amenkiamen (Late), Regional Pastor Chidi Ezimakoh, Pastor Emma Eze, Pastor Joseph Chinedu Ejemba, Pastor Ifeanyi Daberechi, and Pastor Eniwake Orogun, Mrs. Victoria Uchenwaegbulem Okoafor, and Bro. James Ibibor. I say God bless you.

Founding Vice Chancellor and Colleagues at SDU

I am specially indebted to the founding Vice Chancellor of SDU, Professor Jacob Snapps Oboreh and his supportive wife, Prof. (Mrs) Justina Oboreh, for his immeasurable impact in my academic career.

Time will not fail me to extend my deep appreciation to all my academic colleagues in SDU, Ozoro, some of which include: Prof. Ochuko Anomohanran, Prof. Sunny Egboh, Prof. Festus Ibimilua, Prof. Authur Essaghah, Prof. T. F. Adepoju, Prof. C. Ogwu, Prof. E. Ekakitie, Prof.

(Mrs) P. N. Onwuachi-Iheagwara, Prof. A. Agbada, Dr. Ozokeraha (ASUU Chairman, SDU Ozoro), Dr. Kelvin Egberi, Dr. Ufuoma Ugbune, Engr. Dr. Prosper Oghenerukevwe, Dr. James Love Kperegbeji, Dr. Emumejaye Kugbere, Dr. Amos Osakor, and others too numerous to mention. I recognize the immense support from Staff and Students of Faculty of Computing, SDU Ozoro, where I currently serve as the Dean of Faculty; all Nigeria Association of Computing Students (NACOS), SDU Ozoro Chapter.

Professional Organizations and College of Fellows, NCS

I equally appreciate the support of Fellows and members of the Nigeria Computer Society for the professional supports and good counsel in most national assignments and professional events. These include but not limited to the following: Professor Aliyu, Muhammad Sirajo (President of NCS), Samuel Babatunde Ezichi, Mr. Manny Ezecheta, Mr. Prince Majemite, Professor Osofisan, Adenike, Ibrahim Z.B. Tizhe, Professor Chiemekwe, Stella Chinye (formal Vice Chancellor, University of Delta, Agbor), Professor Ejiofor, Virginia Ebere, Professor Asor, Vincent Ele, Dr. Charles Onyeukwu, Rex Ayodeji Abitogun, Leo-Stan Ekeh, Don Etiebet, Mr. Segun Alabi, Professor Jimoh, Rasheed Gbenga, Dr. Okolie, Stanley Adiele, Kenneth Okerieafor, Bayor Mohammed Onimode, Mr. Adebayor Adegbiyi, AVM Victor Udoh and Dr. Vincent O. Olatunji.

Family

I would like to deeply appreciate my parents Chief Sir Engr. Christopher Chinedu Agogbuo, KSM and Lady & Lolo Ezinne Isabel Adaku Agogbuo, for being great support to me through most of my academic and professional pursuit. They laid the foundation of what we are witnessing today. Thank you daddy for all those days when you facilitated and sponsored my research works and publications with the needed moral support; and to my Mummy for motivating and encouraging most great accomplishments in my life even at their incubation stage, thank you is not enough, but God the Almighty will

make up for you two where will failed. I will not fail to appreciate all the unwavering financial, moral and spiritual support of my big sister, Mrs. Precilia Ngozi Ezeliora, who at the shortest notice would always come to my rescue. You are truly a blessing to everyone in your world. The support of my brother (Dr. Michael Okechukwu Agogbuo) and my other sisters (Dr. (Mrs.) Lilian Chidinma Mokwunye and Mrs. Linda Amarachi Egwaoje) are all very much appreciated.

I fondly appreciate my paternal and maternal grandparents, Late Agogbuo Nwaokorie and Esther Agogbuo, and Late Lazarus and Theresa Uzoukwu; my parents-in-law, Late Lazarus Anyile, and Mrs. Comfort Ngozi Anyile. I sincerely appreciate my Uncles and Aunties, Double Chief Martin Uzoukwu, Engr. Reginald Uzoukwu, Rev. Fr. Samuel Kelechi Uzoukwu, Mrs. Patricia Nwanyisunday Okafor, Pharm. Dr. Philomina Uzoukwu, Engr. Dr. Akudo Uzoukwu, Mrs. Gorratti Madumere, and to all my Brothers and Sisters-in-laws including Mr. Victor Ezeliora, Mr. Ugochukwu Mokwunye, Mr. Festus Egwaoje, Dr. Ogechi Agogbuo, Dr. Chioma Dimeke, Dr. Ogechi Isokpehi, Miss Chidinma Anyile, and Miss Chidera Anyile. What much could I have done without you all, and to you I say remain blessed and a blessing to your generation.

My Dear Wife and Children

The popular saying "Behind every successful man, there is a woman" is very true in my life. Ever since I met her, she has remained my strongest pillar of support and closest friend. I wholeheartedly appreciate the unalloyed support of my jewels of an inestimable value, my loving wife Dr. (Mrs) Nkechi Blessing Chinedu. She sacrificed her own progress and advancements for my sake. These were done while she gave maximum support to all family interests and funding to enable me pursue my foreign and local research endeavors, as well as find good footings in my careers both academically and professionally. I couldn't have gotten to this level without your support. Thank you so much for being there for me all the time.

The love, cooperation and support of my admirable and wonderful children (Deborah Chimdiebube Chinedu, David Uchechukwu Chinedu, Daniella Chimnedum Chinedu; whom I fondly called "Original", "Authentic" and "Genuine" respectively) are a major source of inspiration to me and are very much appreciated. My prayer is that you will surpass whatever level I might attain in life in Jesus' mighty name.

Final Thanks

Mr. Vice Chancellor Sir, Finally, as I thank God Almighty, and deeply appreciate everyone who is physically present here today and others who are present virtually, let me end this lecture with this song:

"I AM SAYING THANK YOU JESUS, THANK YOU MY LORD"

Thank you very much for your attention.

REFERENCES

- Al Beshri, A. M. (2013). *Outsourcing data storage without outsourcing trust in cloud computing*. PhD thesis, Queensland University of Technology. Retrieved from <http://eprints.qut.edu.au/61738/>
- Ardagna, C.A., Asal, R., Damiani, E., & Vu, Q.H. (2015). From Security to Assurance in the Cloud: A Survey. *ACM Computing Surveys*, 2. <https://doi.org/10.1145/2767005>
- Bond, J. M. (2015, May 29). The Evolution to Cloud Computing (How Did We Get Here?). *The Enterprise Cloud Blog: Best Practices for Transforming Legacy IT to the Cloud*. <https://mycloudblog7.wordpress.com/2015/05/29/the-evolution-to-cloud-computing-how-did-we-get-here/> Campbell-Kelly, M., Aspray, W., Ensmenger, N., & Yost, J. R. (2023). *Computer: A history of the information machine* (3rd ed.). Westview Press.
- Chinedu, P. U. (2018). *Secured Cloud-Based Framework for ICT Intensive Virtual Organisation*. Approved by: Owerri, Nigeria, Federal University of Technology Owerri, Diss., 2008. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing. ISBN: 978-613-9-82456-4
- Chinedu, P. U., & Hussaini, Y. (2018). ICT Deployment in Governance: A Potent Enabler of Accountability, Reliability and Transparency (ART) of Government Business. *Journal of Engineering Mathematics*, 2(2), 68-78. doi: 10.11648/j.engmath.20180202.13
- Chinedu, P. U., & Nwankwo, W. (2018). Security of Cloud Virtualized Resource on a SaaS Encryption Solution. *Science Journal of Energy Engineering*, 6(1), 8-17. doi: 10.11648/j.sjee.20180601.12

- Chinedu, P. U., & Osuagwu, O. E. (2018). Assessing and Mitigating the Security Concerns, Threats and Associated Risks with Cloud Adoption. *Engineering Mathematics*, 2(2), 95-106. doi: 10.11648/j.engmath.20180202.17
- Chinedu, P. U., Maduabuchukwu, C., Ekruyota, G., Anazia, K. E., Ifeose, & Oyewale, M. A. (2026). Chapter Twenty-Seven - Information Systems Evolution from Centralized Computing Back to the Cloud: A Perspective of SDU 'Digital' Vice Chancellor. In M. Mowarin (Ed.), *Strategic Vision and Ethical Leadership in University Administration: Essays in Honour of Professor Jacob Snapps Oboreh* (pp. 282-294). Hisdeg Global Services Limited. ISBN: 978-978-69-1-889-1
- Chinedu, P. U., Maduabuchukwu, C., Oghorodi, D., & Nazrul Islam, M. S. (2025b). Moving to the Cloud: A Review of the Impact and Strategies for Nigeria Digital Transformation. *Nigerian Journal of Engineering Science and Technology Research*, 11(1), 251-257. ISSN:2315-9073
- Chinedu, P. U., Nwankwo, W., & Eze, U. F. (2013). Enterprise Cloud Adoption: Leveraging on the Business and Security Benefits. *West African Journal of Industrial and Academic Research*, 7(1).
- Chinedu, P. U., Nwankwo, W., & Isong, E. B. (2021). E-Readiness Dimensions for a Consolidated Strategic e-Governance Implementation: The MDA Perspective. *The IUP Journal of Knowledge Management*, 19(2), 46-70.
- Chinedu, P. U., Nwankwo, W., Aliu, D., Shaba, S. M., & Momoh, M. O. (2020). Cloud Security Concerns: Assessing the Fears of Service Adoption. *Archive of Science & Technology*, 1(2), 164-174. ISSN:0189-3548

- Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education (RIGEO)*, 11(7), 956-974. Doi: 10.48047/rigeo.11.07.92
- Chinedu, P. U., Nworuh, G. E., Osuagwu, O. E., & Eze, U. F. (2015). The Security of User Data: Demystifying Fear to Cloud Model and Service Adoption and Deployment. *International Journal of Academic Research*, 7(1).
- Chinedu, P. U., Nworuh, G. E., Osuagwu, O. E., Onyesolu, M. O., & Ahaiwe, J. (2015). Overcoming the Barriers to Enterprise Cloud Adoption within Nigerian Consumer Constituency. *British Journal of Mathematics & Computer Science*, 8(1), 39-56. Article no. BJMCS.2015.143. ISSN: 2231-0851
- Chinedu, P. U., Oghorodi, D., Jeroh, E., Omotosho, S. I., Abah, E. J., Stephen, O. T., Amarime, K., Nwankwo, C. P., & Nwankwo, W. (2025). IoT Adoption in Nigeria's Telecom Sector: Trends, Barriers and Future Prospects. *The IUP Journal of Telecommunications*, 17(1), 467-480. DOI: 10.71329
- Chinedu, P. U., Okeke, C., & Onyeukwu, C. (2018a). The Impact of ICT on National Security: A Case of Nigeria Security and Civil Defence Corps. *International and Public Affairs*, 2(3), 48-61. doi: 10.11648/j.ipa.20180203.11
- Chinedu, P. U., Ugwuegbulam, C., & Akagha, C. (2015). Towards a Cryptographically-Secure Cloud Security Solution. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, 5(1).

- Chinedu, P. U., Yakubu, A., & Osuagwu, O. E. (2018b). An Evaluation of the Impact of ICT on Nigeria Socio-Economic Growth and Development. *West African Journal of Industrial and Academic Research*, 19(2), 139-158.
- Cretu, L. G. (2012). Cloud-based Virtual Organization Engineering. *Informatica Economică*, 16(1). Available from <http://www.revistaie.ase.ro/content/61/09%20-%20Cretu.pdf>
- Ghani, A., Badshah, A., Jan, S. U., Alshdadi, A. A., & Daud, A. (2020). Issues and Challenges in Cloud Storage Architecture: A Survey. *Researchpedia Journal of Computing*, 1(1), 50-65. Doi:10.1109/RpJC.2020
- Harkut, D. G. (2020). Introductory Chapter: Cloud Computing Security Challenges. doi: 10.5772/intechopen.92544
- Hasan, R. (2011). *Security and Privacy in Cloud Computing*. Johns Hopkins University. <https://www.cs.jhu.edu/~ragib/sp11/cs412/lectures/600.412.lecture01.pptx>
- Hellman, M. E. (1980). A cryptanalytic time-memory tradeoff. *IEEE Transactions on Information Theory*, 26(4).
- IBIS TECHNOLOGY (2020). *Demystifying the Fear of Cloud Computing*. <https://ibistechnology.com/demystifying-fear-cloud-computing/>
- IBM Research (2011). *Protocols for Secure Cloud Computing*. Christian Cachin, Zurich. Available: <http://www.zurich.ibm.com/~cca/talks/metis2011.pdf>
- Ike, K. R. (2003). *Introduction to Research Method*. Umuahia, Nigeria: Chudy Publications.

- ISACA (2009). *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives: Emerging Technology White Paper*. <http://www.isaca.org>
- Laudon, K. C., & Laudon, J. P. (2022). *Management Information Systems: Managing the Digital Firm* (16th ed.). Pearson Education.
- Mell, P., & Grance, T. (2023). *The NIST Definition of Cloud Computing* (Special Publication 800-145). National Institute of Standards and Technology.
- Metri, P. et al. (2011). Privacy issues and challenges in cloud computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*, 5(1), 1-6.
- Nwankwo, W. (2020). A Review of Critical Security Challenges in SQL-based and NoSQL Systems from 2010 to 2019. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(2).
- Onatuyeh, E. A., Oghorodi, D., Okpako, E. A., Ojei, E., Osakwe, G., Chinedu, N. B., Okoh, S. K., Odu, V. C., Chinedu, P. U., & Nwankwo, W. (2025). Cybersecurity and Business Survival in Nigeria: Building Customer's Trust. *African Journal of Applied Research*, 11(1), 786-813. ISSN: 2408-7920
- Pedamkar, P. (2023, December 4). Cloud Deployment Models. *EDUCBA Blog*. <https://www.educba.com/cloud-deployment-models/>
- Roy, N., & Jain, R. (2015). Cloud Computing: Architecture and Concept of Virtualization. *International Journal of Science, Technology & Management*, 4(1), Special Issue.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (4th ed.). Essex: Prentice Hall.

Siddiqui, M. (2011). *Cloud Computing Security: Final Paper Submitted Spring 2011*. Available: <http://blogs.techconception.com/manny/content/binary/Manny%20Siddiqui%20%20Cloud%20Computing%20Security.pdf>

SoftwareTestingHelp (2021, January 18). Introduction to Cloud Computing Services. <https://www.softwaretestinghelp.com/cloud-computing-service-providers/>

Tanenbaum, A. S., & Van Steen, M. (2022). *Distributed Systems: Principles and Paradigms* (2nd ed.). Pearson Education.

Ullah, A., Li, J., Shen, Y., et al. (2018). A control theoretical view of cloud elasticity: taxonomy, survey and challenges. *Cluster Computing*, 21, 1735-1764. <https://doi.org/10.1007/s10586-018-2807-6>

UND Blog. (2025). *Computer Science vs Information Technology*. University of North Dakota.

PAST INAUGURAL LECTURES AND DATES

S/N	NAME OF LECTURER	TOPIC	DATE
1	Prof. Jacob Snapps Oboreh Professor of Operations Research and Management	Modelling Account Receivable Risk and Uncertainty: An Approach to Managerial Decision Making	Friday 12th December, 2025
2	Prof. Arthur Efeoghene Essaghah Professor of Urban and Regional Planning	The Designers Portfolio and Next Agenda for Living Cities	Friday 16th January, 2026
3	Engr. Prof. Peters Emuobosa Akpoturi Professor of Petroleum and Gas Engineering	From Source Rock to Revenue: Reservoir Engineering as Pathfinder to Nigeria's Economic Transformation	Friday 30th January, 2026
4	Engr. Prof. Adepoju Tunde Folorunsho Professor of Chemical Engineering	Beyond the Bin: Harnessing Chemical Engineering to Preserve the Earth Through the 3Rs	Friday 13th February, 2026
5	Engr. Prof. Patricia N. Onwuachi-Iheagwara Professor of Petroleum Engineering	Cement Retrogression: Harnessing local additives for its prevention	Tuesday 21st July, 2026



Nigeria we hail thee,
Our own dear native land,
Though tribe and tongue may
differ, In brotherhood, we
stand, Nigerians all are proud
to serve Our sovereign
Motherland.

Our flag shall be a symbol
That truth and justice reign,
In peace or battle honour'd,

And this we count as gain,
To hand on to our children
A banner without stain.

O God of all creation
Grant this our one request,
Help us to build a nation
Where no man is oppressed
And so with peace and plenty
Nigeria may be blessed.



SOUTHERN DELTA UNIVERSITY ANTHEM

O' arise Southern Delta University, Ozoro,
Bearing light of hope and excellence
To lead and dominate the academia
We are a forward, ever moving Institution,
Innovative, creative, taking the bull by the horn,
Brace the future and reach the world
SDU students, leading ever to sing
Let God direct our paths to zenith, With His strength,
We take the world to stardom