International Journal of Library and Information Technology (IJLIT), Vol.2 No.1, March 2022. Pg.1 - 15

SECURITY CHALLENGES OF CLOUD COMPUTING: A CRITICAL REVIEW OF THE NIGERIAN CLOUD COMPUTING POLICY.

GAGA THOMAS ALI,
Department of Computer Science
Bingham University, Karu. Nasarawa State.

&

OBI UCHENNA KIZITO
Department of Computer Science
Bingham University, Karu. Nasarawa State.

ABSTRACT

The Nigerian government through National Information Technology Development Agency(NITDA)put out a cloud computing policy which is expected to ensure a 30% increase in the adoption of cloud computing by 2024 among Federal Public Institutions (FPIs) and Small medium enterprise (SMEs) which provide digital-enabled services to the citizens (Pantami, 2019).

Cloud computing is a growing paradigm that proffers new solutions on ways to deliver computing services and resources over the internet. These services are managed by third parties at remote site and subscribers' pay for services and resources using a pay as you use model.

Information and Communication Technology (ICT) professionals in Nigerian government agencies are concerned with the security challenges of cloud computing and a decline in cloud adoption may prevent the government from taking advantage of the fast-growing technology.

Information gathered from related literature on cloud computing identified security challenges as a major factorlimiting its adoption in Nigeria. The security challenges limiting cloud computing adoption can be categorized into cyber security threats resulting to data loss and violation of privacy,cloud administrator and user account hijacking, lack of Regulatory body to handle cases of accountability between cloud service providers and users.

This research critically reviewed the Nigerian cloud computing policy with regards to security.

The purpose of reviewing the Nigerian cloud computing policy is to identify strategies NITDA used to avoid the security challenges of cloud computing through the cloud computing policy. The United Kingdom (UK) cloud computing policy (one government cloud strategy) was also reviewed to identify strategies used to avoid the security challenges of cloud computing.

NITDA used data classification to implement information security in cloud computing environment. The Nigerian cloud computing policy also highlighted some standard compliance certification for cloud service providers to help enforce security. Data was classified into four categories as regards to security. National security information holds the highest priority while sensitive government or business/citizen data, routine government business data and public or non-confidential data follows with diminishing priority. NITDA categorized classified data into three groups: Routine government business data, sensitive business and citizen data and public/non-confidential data. Protecting this data requires the use of industry standard security on public cloud solutions. Protecting sensitive government or business/citizen data requires the use of a private or hybrid cloud solution with enhanced security controls. Protecting national security information requires custom hardened on-premises systems (local data center).

Review of the United Kingdom cloud computing policy (one government cloud strategy) identified ways used to mitigate the security challenges of cloud computing in the UK, Nigerian cloud policies can be enhanced from the lessons learnt from the UK experiences.

INTRODUCTION

The Nigerian government developed a Cloud computing policy through the National Information Technology Development agency (NITDA) because of its perceived economic and operational benefits. Stakeholders in the digital age believed that cloud technology will transform the IT industry and significantly improve business continuity and quality of service delivery in government organization (Pantami, 2019).
Cloud computing is a new model for provisioning infrastructure services, applications, general computing, and storage resources on-demand (Engel & Lisa, 2014) but there are already known security threats that have exploited the usage of Cloud Computing (Rohan & Jagli, 2017). According to (Uchenna, Godwin, Oliver, & Eze, 2015) securing data stored in cloud explains the fear limiting cloud computing adoption and cloud computing model deployment. Cloud technology is one of the factors leading the 21st-century digital transformation; it provides a holistic platform that enables the use of cyber security, artificial intelligence, big data, digital networking, disaster recovery and backup recovery

WHAT IS CLOUD COMPUTING?

Cloud computing is the use of wide range scalable services provisioned over the Internet (Rohan & Jagli, 2017). It originated from a quest to accomplish a decentralized environment where computing resources would be shared and managed over the internet using advanced virtualization packages and managed hosting infrastructure and services (Engel & Lisa, 2014). The challenges surrounding local data centers led to the reality of cloud computing as the traditional data centers were running at high operational cost and exposed security threats.
(Rohan & Jagli, 2017) classified cloud computing based on two models, service models and deployment models. Services models are generally classified in three categories. Infrastructure-as-a-Service (IaaS), Platform-as-a Service (PaaS) and Software-as-a-Service (SaaS) while deployment models are categorized into public cloud, private cloud, hybrid, and cloud community cloud. The automation and virtualization of these computing services completely abstracts a user from the physical computing environments. This made cloud technology explode in adoption by government organization and private sectors.
(Obodoeze, 2014) defined cloud computing as the use of computing infrastructures and resources (hardware and software) as a service over a network (internet).According to (Engel & Lisa, 2014), cloud computing represents a new paradigm in the evolution of computing and Communication Technology development because it introduced a new type of service which provides an abstraction layer for infrastructure services, virtualization environment, portability, and automatic provisioning.
(Mell & Grance, 2011) defined Cloud computing as a rapidly provisioned model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources released with minimal management effort or service provider interaction. The definition was accepted by the National institute of standards and technology because it demystifies the core components of cloud computing, the definition consists of the following components (see fig. 1):

- On-demand self-service: Today, consumers can easily provision computing resources like network storage, servers, and application programming interface (API) endpoints. This provisioning can be done automatically without intervention from anyone including the Cloud Service Providers (CSPs).
- Resource pooling: The providers put together a pool of computing resources that services the needs of multiple consumers by implementing a multi-tenant model. In this case, different physical resources managed by these cloud service providers (CSPs) are being assigned and reassigned dynamically to different consumers based on their demands. At a higher level, consumers do not know the exact level where these resources are located but can specify an area where they want these resources to be located. This level of abstraction has led to the transformation of the conventional on-premises data center into migrating fully to the cloud or running a hybrid kind of environment.
- Broad network access: Due to the heterogeneous nature of devices that could connect to cloud services, network capabilities are put in place by CSPs to accommodate various devices while keeping to standards.
- Rapid elasticity: Another good area the definition addresses is that the capabilities of these resources can be scaled automatically internally and externally.

In the last ten years, the Nigeria government has created awareness of the importance of cloud computing and developed the needed policies and framework for the full implementation of cloud computing in Nigeria However, the uncertainties around data security complicates firms' adoption of cloud technology (Nicho & Hendy, 2013).
These uncertainties keeps' organizations looped in a decision to adopt cloud computing and thus outsource sensitive corporate data/IT resources to a third-party vendor (Dutta, Peng & Choudhary, 2013).

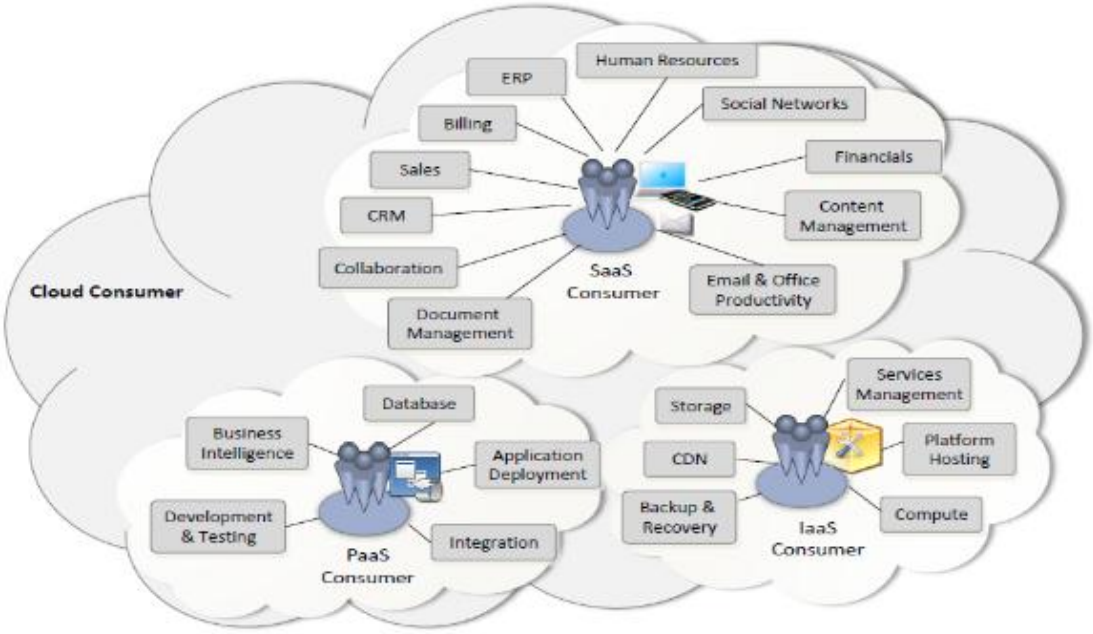

Figure 1: Available services for cloud users. (Source NIST)
The significance and impact of cloud computing are currently being felt in all areas of endeavors in the world. To help guide the implementation of cloud-based services and boost its adoption in Nigeria, the National Information Technology Development Agency (NITDA) released a cloud computing policy that defines boundaries in data management and provides a level playing ground for local cloud service providers.

RESEARCH METHODOLOGY

To carry out this research secondary data was gotten from existing literature, academic journals, existing data on the subject and the Nigerian cloud computing policy.
The research explored a comparative analysis of the United Kingdom cloud computing policy to the Nigerian cloud computing policy to identify gaps and strategies to reduce the security challenges of cloud computing in Nigeria.

LITERATURE REVIEW

2.1 SECURITY CHALLENGES OF CLOUD COMPUTING

Security challenges has been identified as one of the most widespread and crosscutting problems related with cloud computing adoption in Nigeria (Uchenna, Godwin, Oliver, & Eze, 2015). According to (Turab, Taleb, & Masadeh, 2013), the implementation of cloud computing involves three parties. The Cloud Customer (user), Cloud Service Provider CSP and internet (network) connection.

Figure 2: Cloud computing parties**.**

According to (Turab, Taleb, & Masadeh, 2013) security challenges threading cloud computing at CSP level includes Guest-hopping attack, SQL injection, Side channel attack, Malicious Insider, storage security and Address Resolution Protocol (ARP) Cache Poisoning.
Cloud computing depends solely on existing networks infrastructure such as LAN, MAN and WAN so it is exposed to the same security attacks threatening cyber security. Social engineering and phishing are the major security challenge threatening cloud user's domain. Domain Name System (DNS) attacks, Domain hijacking, and IP Spoofing are the major attacks threatening the network domain of cloud computing (Turab, Taleb, & Masadeh, 2013).

(Turab, Taleb, & Masadeh, 2013) concluded that cloud computing is an attractive solution when the infrastructure or the IT personnel are available and not too expensive. However, the drawback is mainly found in the security threats and vulnerabilities unlike the traditional solutions where threats come from two known sources inside or outside the network.

(Tomar, Singhal, & Kumar, 2011) described various security issues that could arise at the Software as a Service (SaaS) domain of cloud computing and their solutions. They discussed Service Level Agreement (SLA), Security management standards, Security Models, and solutions to security challenges. Service Level Agreement is a document between two parties (cloud service provider and cloud service user). This document defines the relationship between cloud service provider (CSP) and the cloud service user. if used properly, it should Identify and define all customer's needs, provide a framework for understanding, simplify complex issues, reduce areas of conflict, encourage dialog in the event of disputes and eliminate unrealistic expectations.

According to (Tomar, Singhal, & Kumar, 2011), Service Level Agreements must discuss how security risks are to be handled when adopting cloud computing models. These risks include Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability. The paper also documented some standards that are relevant to security management practices in cloud. These standards include information Technology Infrastructure Library (ITIL), ISO/IEC 27001/27002 and Open Virtualization Format (OVF).ITIL is based on the code of practice for information security management now known as ISO/IEC 27002 which breaks down information security into policy, processes, procedures, and work instruction.

The location of the data server housing organization information is always unknown to organization when adopting software as a service model. This makes the security of critical data a huge concern to organizations. (Tomar, Singhal, & Kumar, 2011) proposed seven ways to mitigate the security challenges at the software as a service domain. The proposed solution includes the use of a Trusted Third-Party Authentication (TTPA) for storing and retrieving the information, prohibiting untrusted applications when we are storing and accessing critical data on and from cloud database server, making some IT rules and regulation to control the Cloud Service Providers, making sure there are no hidden clause in SLA between cloud service providers and cloud service users, Implement Firewall that restricts traffic using protocols, service port and IP address, Implement K Virtual Private Cloud (VPC) and MAC Level Security.

According to (Rohan & Jagli, 2017), securing the storage of data and networks are the biggest security concerns in Cloud Computing. The security issues of cloud computing discussed are compromised credentials, broken authentication, data breaches, hacked interfaces and API'S, exploited system vulnerabilities, account hijacking, permanent data loss, inadequate diligence, cloud service abuses and DOS attacks. The Security challenges of cloud service and deployment models includes Malicious attacks, Backup and Storage, Service hijacking and VM Hopping, third-party relationships, development life cycle, underlying infrastructure security, cloning and resource pooling, unencrypted data, authentication and identity management and network Issues.

(Popović & Hocenski, 2010) argued that it is very important to take security and privacy into account when designing and using cloud services. They also highlighted ways to mitigate cloud security and privacy issues. It includes:

- The need for corporations or end users to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data.
- Developing a formal charter for the security organization and program that aligned with the strategic plan of organization or company.
- Development of security steering committee whose objective is to focus on providing guidance about security initiatives, incentives and alignment with business and IT strategies.
- Risk management which involves assignment of ownership and custodial responsibilities, identification of data and its links to business processes, applications, and data stores.
- Security awareness, Education and training and Identity Access Management

(Muhammed et al., 2014) research highlighted some challenges on cloud adoption in Nigeria. They include.

- Poor internet service which limited the spread of cloud providers in other areas of Nigeria apart from the big cities of Lagos, Port Harcourt, Abuja, and Enugu. All cloud model is built around the internet and as such unavailability of the internet in some areas has affected the adoption of cloud technology in Nigeria.
- Fear of hackers: The increasing number of internet fraudsters has also created biases in the minds of people in such a way that they believe that once they migrate their data to the cloud, the content is at high risk.
- Lack of technical skills and know-how from the cloud service providers.
- Lack of awareness of cloud services amongst the people.

In another study, (Obodoeze et al., 2014), identified that, security, privacy concerns, lack of internet connectivity, high cost of internet subscription, low-quality data centres, power outages, standardisation challenges and lack of cloud bill from the government to control CSPs domiciled in Nigeria are factors limiting the adoption of cloud computing.

(Otuka et al., 2014) in "The use and challenges of cloud computing by SMEs in Nigeria" identified similar challenges as with (Obodoeze et al., 2014)as the major challenges to cloud adoption in Nigeria. The study identified security, lack of standards, Broadband and bandwidth challenges, cost of cloud implementation, reliability of the vendors and technical knowhow as major challenges. The deviating views according to (Obodoeze et al., 2014) are migration from one cloud provider to the other and data lock-in as additional challenges.

The table below summarises the challenges of cloud adoption in Nigeria according to these works.

	In (Muhammed et al., 2014)	Otuka et al., 2014	Obodoeze et al., 2014
Poor internet service	YES	YES	YES
Data Security	Yes	Yes	Yes
lack of standards	Yes	Yes	Yes
Broadband and bandwidth challenges	Yes	Yes	Yes
technical knowhow	Yes	Yes	Yes
migration from one cloud provider to the other	No	No	Yes
data lock-in	No	No	Yes
Lack of awareness of cloud services amongst the people	Yes	No	No

2.2 CLOUD DEPLOYMENT MODELS, ARCHITECTURE AND TECHNOLOGY.

According to (Muhammed, Zaharaddeen, Rumana, & Turaki, 2015) there are three categories of Cloud architectures. These categories include Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

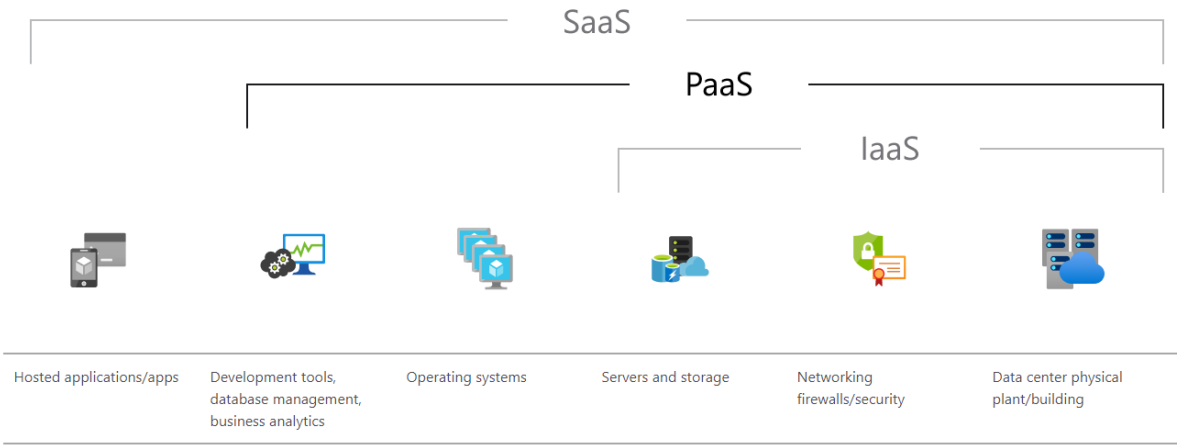

Figure 4: Different types of cloud solution providers (source, Microsoft learn)

2.2.1 SOFTWARE AS A SERVICE

Software as a service refers to software solutions that are offered to customers in a pay-per-use manner. They are deployed as hosted service and accessed over the internet (Srinivas et al., 2012). In cloud computing, SaaS services are owned, managed, and delivered remotely by the cloud service providers. The burden of managing the hardware infrastructure on which the software runs is being lifted from the consumers. Security features, upgrades and overall maintenance of the platform are being handled by the provider. In doing this, the consumer focuses on system usage and efficiency in delivering their goal. With SaaS, knowledge of the infrastructure is not needed. For example, Oracle SaaS Platform allows independent software vendors to build, deploy and manage SaaS and cloud-based applications using a licensing economic model. A demerit to this is that no users can scale at their own will. Example of such a platform is Netflix, Office 365, E-SCAN, and many other pay-per-user platforms that require you to log in and start using their software (Muhammed, Zaharaddeen, Rumana, & Turaki, 2015).

2.2.2 PLATFORM AS A SERVICE

Platform as a Service (PaaS*)* provides clients with access to basic operating software and optional services to develop and use software applications (e.g., database access and payment service). It is a model built upon IaaS which provides developers with a cloud-based environment for developing, testing, running, managing applications as well as eliminate the cost of buying and manage underlying computing infrastructure. Google App Engine is an example of platform as a service. It allows clients to run their web applications (i.e., software that can be accessed using a web browser such as Internet Explorer over the internet) on Google's infrastructure.

In cloud computing, PaaS refers to services rendered to clients by providing them with only the development environment. On this type of service, consumers develop their program of solutions using the platform provided to them by CSPs and deliver these same services to their clients or for their personal use. The CSP has control over the hardware infrastructure, network infrastructure, as well as operating system on which the clients build their solutions. The clients on the other hand have control over the applications that run in the environment. They can upgrade their software at will, add or remove features when they like and provide extended services based on their applications. An example of this type of platform is the Azure SQL Database. With Azure SQL DB, clients can build their software using the azure SQL DB without bothering about the operating system and other components on which azure SQL DB runs. In most instances, this is referred to as a managed instance service(Muhammed, Zaharaddeen, Rumana, & Turaki, 2015).

2.2.3 INFRASTRUCTURE AS A SERVICE

Infrastructure as a Service (IaaS) is the basis of cloud services. It provides access to server hardware, storage, bandwidth, and other fundamental computing resources to clients enable companies to provision virtualized computing resources through the Internet or a dedicated connection. it allows cloud users, businesses, and government organization to rent preconfigured machines with selected operating systems on which they can run applications.

In cloud computing, infrastructure as a service refers to services delivered to customers by offering a virtualized platform for them to build, maintain and deliver their solutions. They do not own the hardware but with the help of virtualization technology, they can control the environment in which they are building their solutions on. Rather than buying servers, storage, networking equipment, cyber security solutions, and data center spaces, consumers buy those resources from a CSP or CSPs as a total package and use them to build and deploy their software or solutions. Consumers are also responsible for security features in their environment. They purchase a firewall of their choice and the operating system they wish(Muhammed, Zaharaddeen, Rumana, & Turaki, 2015).

2.2.3 TECHNOLOGIES POWERING CLOUD TECHNOLOGY.

- Hardware Virtualization: To serve a broad spectrum of consumers, CSPs employ maximum flexibility in providing a virtualized environment for their clients thereby giving them an illusion of dedicated computing, networking, and storage resources. With virtualization, users do not get the feeling of using a public cloud service that runs off hardware. They configure their respective resources as they wish.
- Virtualized Network Block Storage: This technology is like the virtualized hardware file server. It allows easy mounting of storage infrastructure to a virtual machine. It can also be likened to a virtualized file server with redundant capability. Azure Blob storage, Azure data storage and AWS Elastic Block storage are clear examples of this.
- Sandboxing: Sometimes the overhead per virtual machine can be quite significant, as typically each virtual machine is running its kernel instance, (Mell & Grance, 2011)**.** The use of high-level programming languages in building boxes that isolates each customer's virtual machine is known as sandboxing.
- Scalable data store: Scalable data store is one of the important technologies used in building scalable web services as they provide a possibility for databases to manage the data behind web applications.

They scale horizontally or vertically based on the needs of the clients. Unlike the periods where a web application will have to be shut down if it exhausts its storage allocation on the host machines, they automatically scale, and you get billed for it later.

- Cloud Controller: All the cloud providers also make a room for accessibility either through user interfaces or command line. Azure CLI is an example of a typical command-line tool for the creation and deployment of Azure services.

These technologies put together to help cloud providers to deliver various models of cloud solutions to their clients. There are 4 majorly identified models with which cloud providers deploy their services to their clients. One such model is the private cloud model where an organization solely request cloud infrastructure. The hardware components might be owned by the organization or owned by another organization or even a third-party provider. The second one is the community cloud model where a set of consumers or clients comes together to setup cloud infrastructure and share the cost amongst them. They share the concerns of cloud environment in terms of security requirement, policies, and compliance considerations. Public cloud is another model used in deploying cloud solutions. In this case, the cloud infrastructure is provisioned for open use by the public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Hybrid cloud is the final deployment models for cloud infrastructure deployment and management. In this case, it is usually a composition of two or more different cloud infrastructure (public, private or community) that are bound by proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing) (Mell & Grance, 2011).

2.2.4 CLOUD COMPUTING CHALLENGES.

Despite the numerous advantages of cloud computing, a broad spectrum of challenges has been identified from related literature as part of the general challenges which CSPs and governments need to address to grow the adoption of cloud technology in a country. The table below shows a number of these challenges.

Challenges	Brief Description
Lack of Standards	Cloud technology is still at the growing stage; hence, no institution is responsible for defining standards to be followed globally. As a result of this, switching from one cloud provider to the other is a nightmare.
Lack of Regulations	In many countries, regulations governing cloud computing is not clear enough for customers to know their jurisdiction and what to expect from a cloud provider.
Vendor Lock-in	This is a situation whereby a customer gets stuck to one cloud provider because of fear of loss of data. A typical example is the Wix platform that does not offer a data migration option.
Loss of Control	When adopting cloud, organizations fear the loss of control over their IT environment. They depend on SLA fulfilments by the CSPs
Privacy Concerns	Customers are scared whether Cloud providers will let out their data.
Reliability	Cloud computing services are delivered over the internet. Much of the reliability issues come from internet usage. Customers from developing countries facing internet issues tend to see cloud technology as unreliable.

Security Concerns	Most companies out of fear of data loss and cyberattacks prefer to keep their data within their private network. The paradigm shift to a public cloud is now a big challenge as these organizations are finding it hard trusting cloud providers with the security of their data.

3.0 A COMPARATIVE STUDY OF THE NIGERIAN CLOUD COMPUTING POLICY AND UNITED KINGDOM ONE GOVERNMENT STRATEGY

3.1 THE NIGERIAN CLOUD COMPUTING POLICY

Information and Communication Technology policies in Nigeria are driven by regulations from NITDA and National Communication Commissions under the supervision of the Ministry of Communications and Digital Economy.

The Nigerian Cloud computing policy is a strategy document developed by NITDA to aid the adoption and implementation of cloud computing. The strategy targets public institutions, the private sector and Small and Medium Enterprises (SMEs) who provide IT services by providing them with a guide on how to invest in their IT infrastructure while considering the "Cloud-first" approach. The major challenges the Cloud-first policy seeks to address can be summarised into cost, resilient IT, IT scalability, interoperability of platforms, and CSP competition. The Nigerian cloud adoption policies made a clear indication of certifications required for CSPs. It also made provision for the workforce training to spur the adoption of the cloud. It made suggestions to interoperability requirements, data classification and information security, cloud service migration and compliance to Service Level Agreements (SLAs).

3.1.2 STRATEGIES THAT ADDRESSES THE SECURITY CHALLENGES OF CLOUD COMPUTING

3.1.2.1 IMPLEMENTING DATA PRIVACY AND SECURITY

To address possible data security and privacy issues that may arise with cloud computing services, the Nigerian cloud computing policy stated that NITDA will work with government entities to identify strategies that would help find a balance between local content requirements, privacy, security, and intellectual property of national data. NITDA also specified that agencies that wish to process or stored cloud information in jurisdictions with different privacy and information protection laws from those in Nigeria must do so in line with the requirements of Nigerian Data Protection Regulations. NITDA will also provide guidance to Federal Public Institutions to determine which jurisdictions their data may transit or be stored in.

3.1.2.2 DATA CLASSFICATION AND INFORMATION SECURITY

Data classification will be used to implement information security when migrating data of Federal Public Institutions to the cloud. Data would be classified into limited sensitivity, moderate sensitivity, sensitive, and classified or national information. Data with limited sensitivity are official, public, or non-confidential. Moderate data are Confidential, routine government business data. Sensitive data are Secret sensitive government or citizen data. Classified data are National security information. Data with limited and moderate sensitivity are to possess standard security and can be stored in a public cloud environment with identified appropriate. Sensitive data are to have enhanced security controls and National information is to have customized hardened on-premises security control measures. NITDA also suggested a private cloud options for the storage of National information and all data should be stored in Nigeria. The policy also recommended that internal agency policies should be implemented to ensure security of data. At a minimum this shall include information security awareness training for employees and contractors and encryption of data at rest and in motion. To protect consumers, NITDA will work on a framework for executing contracts between Federal Public Institution and Cloud Service Providers.

3.1.2.3 CERTIFICATION PROGRAMS FOR CLOUD SERVICE PROVIDERS

The policy highlighted that it is a cloud service provider's (CSP) obligation to protect its cloud system, the confidentiality, integrity, and availability of its data. The policy stated that Cloud service providers (CSPs) servicing Public Institutions must compliant with the cloud security certification programs that the Nigerian government will establish and NITDA will develop a cloud computing code of conduct.

3.1.3 CRITIC OF THE NIGERIAN CLOUD COMPUTING POLICY WITH REGARDS TO THE SECURITY OF CLOUD SERVICE MODELS

3.1.3.1 SOFTWARE- AS- A- SERVICE

The NITDA cloud computing policy addressed the issues of data security, privacy, and access in cloud user domain. However, there were no clear suggestions on how to address security challenges that may occur within the networking environment of cloud computing.

3.1.3.2 PLATFORM-AS-A-SERVICE

The policy made no suggestion or recommendation on how to manage the security challenges that may occur within the network domain of cloud computing.

3.1.3.3 INFRASTRUCTURE-AS-A-SERVICE

The Nigerian cloud computing policy highlighted the use of standard cloud security certification by CSP to ensure security. However, the policy made no suggestion or recommendation on how to manage the security challenges that may occur within the network domain of CSP cloud service providers.

3.2 THE UNITED KINGDOM (UK) ONE GOVERNMENT CLOUD STRATEGY

Improved security and good service delivery are the outcomes of well-implemented cloud technology. Hence, government institutions must work closely with each other to explore the full benefits that come with cloud technology. To do this, the government of the UK brought together representatives of digital transformation from various government organizations to help draft a service delivery model that focuses on how the public can benefit and getting the best value from cloud computing. This led to the drafting of a guide known as "The One Government Cloud Strategy (OGCS)". The one government cloud strategy addresses issues like vendor lock-in, technical, commercial, security and operations related issues. The multi-functional approach taken by the government in bringing Chief Information Officers of different organizations together was a great step as it helped the government to draw out plans that fit into different scenarios or organizations. The OGCS recommends the cloud-first policy which suggests that when procuring new or existing services, the public sector should consider public cloud solutions first before considering other alternative options (*Government Cloud-First Policy - GOV.UK*, n.d.). The cloud-first policy regards the public cloud first rather than other cloud deployment methods like the hybrid, community, and private cloud. It also suggests that government-owned institutions should consider the Software-as-a-Service model when procuring software solutions.

To help organizations with proper guidelines, the government of the UK gave four strategic areas in (*Cloud Guide for the Public Sector - GOV.UK*, 2020) where institutions need to focus on to get more benefits from a cross-functional or multi-disciplinary team. This includes:

- Digital and Technology: Which is responsible for the building and managing of cloud estates and offering the best technical advice,
- Commercial: Which is responsible for negotiating with cloud providers and managing the relationship with them,
- Security: This is responsible for the continuity of the quality of services by making sure that networks, systems, and data are not exploited,
- Human Resources: Which is responsible for recruiting and development of new and existing staff in cloud technology.

Another area of the OGCS submission is defining a strategy for choosing a hosting platform. In (*Creating and Implementing a Cloud Hosting Strategy - GOV.UK*, 2020), a problem first and strategy second approach is stipulated. This is a method whereby before choosing a cloud model, the tentative problems you wish to solve and the problems that you might face with the cloud model is defined then followed with the strategies of resolution.

Other areas of the OGCS include a guideline for assessing the commercial use case of cloud according to the organization's business case approval process. This stipulates some contract agreement processes and data retention policy by third parties. It also recommends the use of Memorandums of Understanding which defines the baseline for technical, security, commercial and legal principles across government institutions and the cloud service providers. Finally, OGCS also provided a guide for managing costs, off-shore and data residency, the security of data centres and data according to the stipulations of the National Cyber Security Centre (NCSC), the migration of legacy solutions and a framework for re-skilling of staff.

3.2.2 STRATEGIES THAT ADDRESSES THE SECURITY CHALLENGES OF CLOUD COMPUTING.

The National cyber security centre report on cloud computing and data storage specified approaches, descriptions, and guidance on ways to implement security in cloud environment using 14 consultation principles. These principles include protection of data in transit, asset protection and resilience, separation between users, government framework, operational security, personal security, secure development, supply chain strategy, secure user management, identify and authentication, external user interface protection, secure service administration, audit information of users, and secure use of the service.

The first principle on the United Kingdom one government strategy is protecting data in transit.

Approaches, description, and guidance highlighted in the one government strategy for protecting data in transit include the shown in the table below:

APPROACH	**DESCRIPTION**	**GUIDANCE**
Private WAN service	You access the service via a private WAN circuits offered by a telecommunications provider. Privacy between different customers of private WAN services is typically by virtue of the routing protocols used, such as MPLS.	Using private circuits will make it more difficult for an attacker to gain access to communications. These connections do not normally provide cryptographic protection but are likely to be hard to intercept and process, which may be adequate for organization's needs. Cryptographic protections, should you choose to deploy them, would provide greater confidence in the protection of the confidentiality and integrity of your communications. Public sector organizations can procure circuits which connect to the Public Services Network (PSN). This WAN, and the providers who give access to it, have had their services assessed against the CESG Assured Service (Telecoms) scheme.
Legacy SSL and TLS	The service is accessed using SSL or legacy versions of TLS.	Use of SSL or TLS versions earlier than version 1.2 is not recommended. There are known vulnerabilities in protocols which

		could be manipulated by an attacker to access data.
TLS	Use of TLS, configured to use cipher suites and certificate sizes	The lack of formal assurance in TLS implementations means there may be implementation weaknesses. Using recent, supported and fully patched versions of TLS implementations from reputable sources will help to manage this risk.
IPsec or TLS VPN gateway	The service exposes a TLS or IPsec VPN Gateway which can be configured to support a strong cryptographic profile.	See our advice on IPsec and TLS configuration to ascertain whether the gateway supports a good profile. Also, a list of VPN products which have been assessed against our Commercial Product Assurance scheme is available here
Bonded fiber optic connections	Bonded fiber optic connections between physically protected locations can be used to provide private connections between data centers.	Independent validation of the service provider's implementation of their bonded fiber optic connections by a recognized expert is advisable. Note that the security of these links is dependent on effective monitoring - this should be one of the considerations for any independent validation of the security provided.

4.0 DISCUSSIONS

The Nigerian government through NITDA could upgrade or develop a cloud guide on how to configure, deploy and use cloud service securely for Federal Public Institutions (FPIs) and Small medium enterprise (SMEs) just like the United Kingdom where they used 14 principles.

The shared nature of cloud resources makes it an attractive target to hackers. Though, NITDA has played a great role in developing a policy for the adoption of cloud computing in Nigeria. However, the cloud computing policy can be reviewed to address the security challenges limiting the adoption of cloud computing in Nigeria. Cloud security and data privacy are considered the major security challenges of cloud computing.

Developing a cloud computing implementation guide like that of the United Kingdom would help achieve a robust cloud computing strategy where government organizations would be aware of real time cloud computing threats, vulnerabilities, and ways to implement security measures to avoid threats and vulnerabilities when using the different cloud computing service models.

The review of the cloud computing policy should focus on the following areas:

SOFTWARE AS A SERVICE SECURITY CHALLENGES

- Authentication and authorization
- Data confidentiality
- Information security

PLATFORM AS A SERVICE SECURITY CHALLENGES

- Duplication of data.
- Privileged debugging access.
- Distributed system computing.

INFRASTRUCTURE AS A SERVICESECURITY CHALLENGES

- Security threats from system hosting virtual machines.
- Security threats from another virtual machine running on the same server.
- Networks & Internet Connectivity attacks (cyber-attacks).

Mitigating threats from systems hosting virtual machines (host systems) involves monitoring virtual machine from host and securing the communication between virtual machine and host.
Cloud infrastructures as a service subscribers' controls, monitor and communicate with virtual machines applications when it's running (on live). Data transferred between virtual machines and host systems are routed through shared virtual resources. Host systems can monitor network traffic of virtual machines hosted on them, start, shut down, pause, and restart virtual machines (VMs) and configure CPU, memory disk, and network usage, view, copy, and modify data stored on virtual disks. This creates exploitable vulnerabilities for hackers to enable data transfer by attacking the internal buffer storage or clipboard of host system or performing a denial-of-service attack. Hence, there is a need to repressively protect host machines more than Virtual machines because authorized users with privilege control to backend computing may misuse these features.

5.0 CONCLUSION

Further research should identify specific security challenges limiting cloud adoptions in Nigeria and prepare a cloud computing guide prototype using real life event as case studies to help avoid the security challenges of cloud computing.

REFERENCES

Al-Isma'Ili, S., Li, M., Shen, J., & He, Q. (2016). Cloud computing adoption determinants:
An analysis of Australian SMEs. *Pacific Asia Conference on Information Systems, PACIS 2016 - Proceedings.*
A., P. (2000). Technology Readiness Index (TRI): A Multipleitem Scale To Measure Readiness To Embrace New Technologies. *Journal Of Service Research*, *2:307*(May).
Baker, J. (2018). *oo f re ct Pr*. *November*. https://doi.org/10.1007/978-1-4419-6108-2
Bel, J. L. Le. (2006). *Article information :*
Bakare, A. (2020). *The Challenges of Adopting Cloud Computing in Nigerian Government Organizations.* Minneapolis: Walden Dissertations and Doctoral Studies; Walden University.
Cloud guide for the public sector - GOV.UK. (2020, March 22). Guidance Cloud Guide for the Public Sector. https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector
Creating and implementing a cloud hosting strategy - GOV.UK. (2020). https://www.gov.uk/guidance/creating-and-implementing-a-cloud-hosting-strategy
Dutta, Peng & Choudhary. (2013). Risks in Enterprise Cloud Computing: The Perspective of it Experts. *Journal of Computer Information Systems*, 39-48.

Engel, L. (2014). Cloud Computing Definition, Ref Architecture, & General Use Cases Transcript. *IEEE*, 1-23.

Eveland, J. (2016). *Technological Innovation as a Process*. *January 1990*.

fusch, P., & Ness, L. (2015). Are We There Yet? Data Saturation in Qualitative Research. *The Qualitative Report*, 1408-1416.

Government Cloud First policy - GOV.UK. (n.d.). Retrieved January 28, 2021, from https://www.gov.uk/guidance/government-cloud-first-policy

Government of Canada Cloud Adoption Strategy: 2018 update - Canada.ca. (n.d.). Retrieved January 22, 2021, from https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html

Government of Canada Right Cloud Selection Guidance - Canada.ca. (n.d.). Retrieved January 24, 2021, from https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-right-cloud-selection-guidance.html

Hentschel, R., Leyh, C., & Petznick, A. (2018). Current cloud challenges in Germany: the perspective of cloud service providers. *Journal of Cloud Computing*, *7*(1). https://doi.org/10.1186/s13677-018-0107-6

Loske, Widjaja, Benlian, & Buxmann. (2014). Perceived IT security risks in cloud adoption: the role of perceptual incongruence between users and providers. *Twenty Second European Conference on Information Systems*, 276 - 296.

Mathew, N., & Mahmoud Hendy. (2013). Dimensions Of Security Threats In Cloud Computing: A Case Study. *Review of Business Information Systems*, 4-21.

Muhammed, K., Zaharaddeen, il, Rumana, K., & Turaki, A. M. (2014). Cloud Computing Adoption in Nigeria: Challenges and Benefits. *International Journal of Scientific and Research Publications*, *5*(7), 2250–3153. www.ijsrp.org

National Bureau of Statistics. (2019). *Nigerian Gross Domestic Product Report.* Nigeria: National Bureau of Statistics.

Nicho & Hendy. (2013). Dimensions Of Security Threats In Cloud Computing: A Case Study. *The Clute Institute*, 159-170.

NITDA. (n.d.). *Background – NITDA*. Retrieved January 16, 2021, from https://nitda.gov.ng/background/

NITDA. (2019). *Nigeria Cloud Computing PolicyNo Title*. 1–33.

Obodoeze, C. F., Okoye, F., & Asogwa, T. C. (2014). Cloud Computing in Nigeria: Prospects, Challenges and Operation Framework. *International Journal of Engineering Research &Technology (IJERT)*, *3*(6), 2107–2113. http://www.ijert.org/view-pdf/10402/cloud-computing-in-nigeria-prospects-challenges-and-operation-framework

Oguntala, G., Abd-Alhameed, P. R., & Odeyemi, D. J. (2017). Systematic Analysis of Enterprise Perception towards Cloud Adoption in the African States: The Nigerian Perspective. *The African Journal of Information Systems*, 213 - 229.

Otuka, R., Preston, D., & Pimenidis, E. (2014). The use and challenges of cloud computing services in SMEs in Nigeria. *Proceedings of the 8th European Conference on Information Management and Evaluation, ECIME 2014*, *January 2014*, 325–332.

Palinkas, L., Sarah, H., Carla, G., Jennifer, W., Naihua, D., & Hoagwood, K. (2013). Purposeful Sampling for Qualitative Data Collection and Analysis. *Administration and Policy in Mental Health and Mental Health Services Research*, 533-544.

Popović, K., & Hocenski, Ž. (2010). *Cloud computing security issues and challenges.* Croatia: Institute of Automation and Process Computing.

Rohan, J., & Jagli, D. (2017). Cloud Computing and Security Issues. *Journal of Engineering Research and Application*, 31-38.

Turab, N. M., Taleb, A. A., & Masadeh, S. R. (2013). CLOUD COMPUTING CHALLENGES AND SOLUTIONS. *International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5*, 209 -216.

Uchenna, P., Godwin, N., Oliver, O., & Eze, U. (2015). The security of user: Demystifying fear to cloud model and service adoption and deployment. *International Journal Of Academic Research*, 223-233.

What Are Cloud Policies? | CloudHealth by VMware. (n.d.). Retrieved January 16, 2021, from https://www.cloudhealthtech.com/blog/what-are-cloud-policies