VOLUME 6 ISSUE 2, 2021

ENUGU STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
TECHNOLOGY FOR SERVICE

# Journal of Social Sciences

Published by
Faculty of the Social Sciences
Enugu State Unviersity of Science & Technology
www.esutjss.com

ENUGU STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
TECHNOLOGY FOR SERVICE
Journal of Social Sciences
Published by the Faculty of the Social Sciences

# Biometric Information Management in Nigeria: A Case of National Identity Management Commission

**Fidelia Nebechi Onuigbo**
Department of Economics
Enugu State University of Science & Technology
Enugu, Enugu State, Nigeria
*ifeifeonuigbo@yahoo.com*

## Abstract

*This research work examined the use of information communication technology (ICT) in information management in Nigeria using the National Identity Management Commission. The study submitted that for government to fulfil their non-negotiable functions, ICT is a necessity. The data used in this study was collected from secondary sources. The secondary sources of data collection included textbooks, journals, government publications and internet sources. The data analysis revealed that ICT usage will enhance NIMC biometric activities. Biometrics offers usability advantages over traditional token and password based authentication schemes, but raises privacy and security concerns. When compromised, credit cards and passwords can be revoked or replaced while biometrics are permanently associated with a user and cannot be replaced.This study concluded that since a sound national identity management system is linked with and complements the development of the socio-political and socioeconomic processes, there is therefore the need for government to facilitate the process for an effective national identity management; and the national identity management policy should be sustained irrespective of changes in government.*

**Keywords**: Biometrics, identity and identity management, national security and Nigeria.

## Introduction

All organisations have a non-negotiable predetermined objective of functioning effectively as well as efficiently. One of the reasons is for the sake of continuity and cohesion. This applies to local governments. Speaking more critically, the continuity of any organisation depends on how innovative that organisation is. Innovation here entails the introduction of new ideas and ways of doing things. If such organisations do not seem to be innovative as to change positively with the changing times, they seem to lose their cutting edge as well as their competitive advantage not to mention their service capacity. Thus, it is truism to state categorically that aside the financial and material resources factor, innovation is centrally responsible for the efficiency and effectiveness of organisations (Zhang, 2019).

Innovation, which is a necessity, is the mother of invention and innovations cannot be exhaustively talked about without the mention of information communication technology. Information communication technology (ICT) is a relatively modern invention as in time past, some less sophisticated and more crude paraphernalia has been used generally by people and organisations alike.

Within the last decade, there has been an unprecedented leap and growth in the application of new technologies in organisations to the extent that organisations that use such modern technologies are christened ‘modern organisations’. These modern organisations overtime, have been able to make reasonable headways remotely and immediately as a result of the application of the tenets and doctrines of Information Communication Technology. A reasonable percentage of such organisations that utilise ICT techniques are private organisations. Thus, the question of ‘what about the public organisations?’ becomes a very wise question to ask.

Any organisation without a well-equipped and updated information technology is more or less a dead one if not passive. Thus, information technology is the blood that flows in and through the veins of any modern organisation without which any other activity whether embodied in human resources, financial resources, information resources etc. will be poorly managed, objectives not considerably achieved, communications truncated and abated and overall efficiency cum effectiveness goal, defeated. Hence, if only a low amount of public setups use ICT principles and innovations, or if at best they use it in a low capacity, what will be their fate? Public setups even as the name suggests has a ‘people’ orientation i.e. its impact is people centred and thus its activities will definitely rub off on the people/masses.

Therefore, ICT use and application is of paramount necessity to public organisations as well as private institutions. Coming from another standpoint, ICT usage in the public sector has however recorded a fairly significant success as a result of its mediocre usage especially at the broader levels of government i.e. the federal and even the state level. But the same, unfortunately, cannot be spoken about the local/grass root level. A typical analogy was a case situation where an assignment given, entailed getting the internally and externally generated revenue of six local governments. This entailed an uphill task of going to the individual local governments umpteen times after which old files which were hitherto dumped were exhumed. The sorting of these files was a different tale in volumes altogether. Instead of an academic lift through the information to be gotten, we became utterly bamboozled as a result of the haphazardness of the whole process. The point being made here is that if this research work was state centred or even federal centred, the answers would have been just clicks away on the computer. This goes to show how rudimentary the local governments are in the use of ICT principles.

Biometric data is important for planning and development. In Nigeria, it has expended millions of naira to gather the biometrics data of Nigerians. But due to lack of coordination, each of these agencies preferred to initiate their own biometric data gathering process. These have led to multiple organizations doing the same thing. In view of the above background, this study seeks to examine the use of information communication technology (ICT) in information management in Nigeria using the National Identity Management Commission. To achieve this objective, the study is divided into five sections. Following section one is the conceptual issues/theoretical framework presented in section two, section three is the methodology/research design. Section four discuss the findings/results and section five presents the conclusion and policy recommendations.

Biometrics is an automated methods of recognizing a person based on a physiological or behavioural characteristics. They include face, finger print, hand geometry, hand writing, iris, retina, vein and voice-anything that is a part of your (Jay & Dunphy, 2009). They further stressed that biometrics is not a new technology. The ancient Egyptians used bodily characteristics to identify workers to make sure they don’t claim more provisions than they were entitled just like governments today are using biometrics to lessen fraud. Chinese Merchants in the fourteenth century used palm prints and fort prints to identify children. Finger print recognition is by far the most developed technology today. It’s trusted, lost effective and easy to use. All biometrics has strengths and weakness. The key is finding the right technology for the right application.

Biometric technologies don’t conjure up the fears they used to overall acceptance of biometrics has risen substantially over the years due to the aftermath of the proliferation of identity theft, technology improvements, and general understanding and awareness. Of course, some people still object at the mention of system that scan fingerprints, but for the most part, people now understand that biometrics actually protect their privacy and that in most biometric applications, their fingerprints are not stored anywhere and their fingerprints can never be recreated from the encrypted digital template (Bovens, 2005).

Biometrics involves collection of finger prints of individual for correctly identifying the real person in a transaction and to avoid frauds and identity thefts, as no two persons in the world have similar fingerprints, even Siamese twins. However, the use of technology for accurate identification of persons to check frauds and make easy the ways of doing things in civilized world has been turned an into instrument of oppression in Nigeria, which is why nothing works, expect corruption, the nation's thriving industry.

The Bank Verification Number (BVN) is a Biometric registration of customers in the financial system. Its introduction is intended to tackle cybercrime and ATM fraud. The central bank verification number allows customers to have "a single identity within the financial system". Thus, people who are unable to read and write will be able to use their biometrics for banking transactions, as this cannot be replicated. It will tackle incidents of identity theft and enable banks to verify their customers easily and, in the longer term, the African banking industry. The Biometric Verification Number (BVN) was conceived to address his identification challenge. The idea is very simple. Capture the finger prints and picture of ever bank customer and save the information with a number, which can then be issued to the customer and can be used to verify his/her identity.

The way the technology works is straightforward. CCTVs in streets, public places, and office buildings record images 24/7, sophisticated algorithms then carry out a matching exercise with an existing database of images of potential "villains" or "targets." A match will trigger enhanced surveillance and possible future and further action. For the system to be effective, the matching database should be as wide and comprehensive as possible. It is not surprising to note that to put such a database together security agencies never (at least we cannot identify any evidence) consult or seek permission to keep people's records in their data centers. Furthermore routine phishing activities through the Internet and social networks provide a fertile ground for not only a simple one-dimensional set of data (photos and other personal data) but potentially three-dimensional datasets of associated friends, links, habits, and quite often current location.

The security of the biometric authentication data is vitally important, even more than the security of passwords, since passwords can be easily changed if they are exposed. A fingerprint or retinal scan, however, is immutable. The release of this or other biometric information could put users at permanent risk and create significant legal exposure for the company that loses the data. At the end of the day, every company is responsible for its own security decisions. You cannot outsource compliance, but you can reduce the cost of compliance, and the possible repercussions of a leak, by picking the right vendor. If a small or mid-sized company uses, say, Google’s or Apple's authentication technology and there is a security breach with Google or Apple, it is likely Google or Apple will get the blame.

In Nigeria, your National Identification Number (NIN) is used to tie together all records about you demographic data, fingerprints, head-to-shoulder facial picture, other biometric data and digital signature in the National Identity Database making it relatively easy to confirm and verify your identity when you engage in travels and transactions. An individual’s fingerprints, passport photo, signature, biometric and demographic data are all linked together in the National Identity Database via his/her NIN. This vital feature of the NIN makes it pivotal for all citizens (home and abroad) as well as legal residents of Nigeria to endeavour to obtain their unique NINs as soon as they can. The Agency that is responsible for collecting these records is the National Identity Management Commission (NIMC), Nigeria’s agency charged with handling digital identity issues, has been called upon to accelerate the process of establishing biometric digital identification for citizens of the country of more than 200 million people.

## The National Identity Management Commission (NIMC)

The trajectory of the national identity management system in Nigeria dated back to the post-independence era (Musa, 2000). For more than four decades, the development of a framework for identity management system has always seamlessly emerged in the government agenda for socio-economic and political development in Nigeria.

In 1978, the Directorate of National Civic Registration (DNCR) was established (Ayamba and Ekanem, 2016). This was later backed by decree 51 of 1979. The DNCR was responsible for the enrollment of citizens from 18years above for National Identity Card (Vanguard May 13, 2003). The government intended to establish a national identity management system to resolve the challenges of verifying and authenticating the true identity of individuals when accessing public service deliverables (NIMC, 2013).

Consequently, a series of government programmes aimed at installing a reliable identification system has always witnessed drawbacks of varying magnitude. Among these drawbacks are fragmented systems, multiple forms ofID cards, non-existence of interoperability, low coverage and absence of common standards as part of the blight that confronted previous identification schemes (Aliyu, 2017). As a result of these ignoble realitiesthe government commissioned a Harmonization Committee to advise it on how different public and private sector activities on identification systems can be harmonized, therefore, the committee recommended a National Policy and Institutional Framework for a National Identity Management System for the country (Ayamba & Ekanem, 2016, p.280).

The national policy and institutional framework for an identity management system for Nigeria was deployed in 2007with the overriding policy thrust to harmonize existing identification schemes, introduce a unique national identification scheme, institutionalize a system of identity management, and establish a reliable environment of identity management. All these thrusts are expected to manifest into attainment of a variety of the policyobjectives set out in the policy documents especially in the area of interoperability among government agencies.Going by the foregoing, the new identification system in Nigeria is expected to provide a foundational database that can be accessed by government agencies providing e-services. However, available evidence raises concern.

For instance, the policy targeted the distribution of at least 12 million NINs to Nigerians in the first year of implementation. Eventually, World Bank Report on the country assessment of the identification system observed that the first National Identification Number was first issued in 2012, four years after commencement of the policy (World Bank,2015). The report also revealed that only 6.1millions NINs were issued to Nigerians representing 3.5% of the total population of Nigeria in 2015. Also, as of September 2017, 21millions NINs has been issued against an estimated population of over 180 million persons in Nigeria equating 12% of the population. Also, it is reported that the National Identity Management Commission operates 805 registration centres out of which 556 centres are located in local governments (NIMC's Official Release, 2017).

The National Identity Management Commission (NIMC) established by the NIMC Act No. 23 of 2007, the NIMC has the mandate to establish, own, operate, maintain and manage the National Identity Database in Nigeria, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to those who are citizens of Nigeria as well as others legally residing within the country.

The NIMC Act 2007 provides for the establishment of the NIMC, its functions, powers, establishment of the National Identity Database, assignment and use of General Multi-purpose cards, and the National Identification Number (NIN). The Act also provides the Commission with powers to make regulations connected with its functions. The NIMC Act 2007 provides the repeal of the law that created the former Department of National Civic Registration (DNCR) and the transfer of its assets and liabilities to the NIMC.

**T**he National Identity Management Commission is the primary legal, regulatory and institutional mechanism for implementing Government's reform initiative (in the identity sector) as contained in the National Policy and NIMC Act, Sections 1, 2, 5 and 6. With this Act, it was able to wind up and take over the assets and liabilities of the former DNCR which no longer exists, including the personnel in both the State and Local Government Offices nationwide. With this mandate, it became imperative that it should establish, operate and manage the National Identity Management System (NIMS): Carry out the enrolment of citizens and legal residents as provided for in the Act, Create and operate a National Identity Database, Issue Unique National Identification Numbers to qualified citizens and legal residents and f**oster** the orderly development of an identity sector in Nigeria. Issue a National Identity Smart Card to every registered person 16 years and above, Provide a secure means to access the National Identity Database so that an individual can irrefutably assert his/her identity [Person Identification Verification Services (PIVS) Infrastructure]. Her vision and mission statement is to provide sustainable world-class identity management solution to affirm identity, enhance governance and service delivery in Nigeria and to establish and regulate a reliable and sustainable system of National Identity Management that enables citizens and legal residents affirm their identity in an environment of innovation and excellence.

Section (6) of the NIMC Act No. 23 of 2007 outlines that the Commission shall have power to:

*Request for any information on data from any person on matters relating to its functions under this Act;*

*Fix the terms and conditions of service including remuneration of the employees of the Commission;*

*Establish and operate administrative and monitoring offices in the States, Local Government Areas and Area Councils;*

*Monitor any matter that may affect the functions of the Commission;*

*Do such other things which this Act or any other enactment are required or permitted to be done by the Commission.*

The functions of the Commission are contained in Section 5 of the Act. Section (5) of the NIMC Act No. 23 of 2007 stipulates that the Commission shall:

*Assign a unique National Identification Number to any person registered pursuant to paragraphs (b) and (c) of this section and the National Identification Number shall be incorporated into or made compatible with other existing identity related databases or registers in respect of which information or data relating to the registered person has been registered, documented or stored;*

*Create, manage, maintain and operate the National Identity Database, established under section 14 of this Act including the harmonization and integration of existing identification databases in government agencies and integration of existing identification databases in government agencies and integrating them into the National Identity Database;*

*Collaborate with relevant bodies and agencies in setting of standards and technical specifications for telecommunications links between organisations and for the devices utilized for such communications established or maintained pursuant to paragraphs (j) and (k) of this section;*

*Collaborate with relevant bodies and agencies in the setting of standards and technical specifications for ICT links between organizations and for the devices utilized for such communications established or maintained pursuant to paragraph (i) and (j) of this section;*

*Maintain secured communication links with end users in any public or private organisation, agency or body including Card Acceptance Devices, Government Service Centres;*

*Perform such other duties which, in the opinion of the Commission, are necessary or expedient for the discharge of its functions under this Act;*

*Collate information obtained by the Commission in pursuance of its functions as stated under the Act and reproducing such information as may be required, from time to time;*

*Ensure the preservation, protection, sanctity and security (including cyber-security) of any information or data collected, obtained, maintained or stored in respect of the National Identity Database;*

*Enter into any form of agreement with any private or public sector based agency or organisation for the development or establishment of the Identity Management Solution or for the realization of any of its functions;*

*Establish and maintain secured communication links with any existing relevant identity related database or agency;*

*Carry out the registration of citizens of Nigeria into the National Identity Database;*

*Carry out the registration of non-citizens of Nigeria who are lawfully resident in Nigeria;*

*Issue a General Multi-purpose Identity Card to any person registered pursuant to paragraphs (b) and (c) of this section;*

*Respond to verification enquires regarding the identification of individuals;*

*Research and monitor developments in the identity management sector;*

*Carry out the registration of births and deaths in Nigeria;*

**The National Identification Number (NIN) Registration Process**

NIMC started enrolment and issuance of NIN since the year 2012 (over nine years ago), and our enrolment and registration centres have been functional and open all year round to provide identity services to the general public. It is quite unfortunate that a large number of citizens and legal residents did not take advantage of those years to enrol for their NIN.

First, the NIN-SIM integration is a policy of the Federal Government of Nigeria through the Ministry of Communications and Digital Economy, due to the improper registration of SIM. So, the directive by the Minister of Communication and Digital Economy to link SIM with NIN was in compliance with the NIMC Act 2007, and Regulations 2017, which stipulate mandatory use of the National Identification Number (NIN) as a valid means of identification for service delivery in Nigeria.

One can see how important the NIN is to an individual:

- it is used for retrieving your captured information from the National Identity Database
- your matching information associated with your NIN can be then used to verify that you are really who you say you are.

To the society as a whole, the NINs issued

- help provide accurate records about actual living/dead persons in every region of the country

- help keep track of actual transactions as well as movement of people within and out of the country
- help confirm which individuals are in actual need of particular Government services, e.g. age and retirement confirmation for pensioners.

When it comes to access to vital services (like passport issuance, banking services, land transactions, insurance services, pension, health insurance, payment of taxes, voter's registration, consumer credits, and all Government services), your NIN becomes necessary for:

- cutting down the time needed for verifying documents to properly identify you in order to access the services you require
- reducing errors in allocation of services to the right people
- prevention of fraud (419) where someone else impersonates you
- verification of the real identity of other people you go into financial or business transactions with or even people you wish to employ such as house help
- ensuring you are properly identified when receiving health services, e.g. verifying the actual blood types of blood donors at hospitals
- verification of voter eligibility during elections.

The ongoing database harmonization efforts with other agencies and banks across Nigeria, with the announcement by the Nigeria Immigration Service making the NIN a requirement for obtaining a travel passport, further emphasize the importance of every individual having his/her ownNIN.

Eventually all agencies and banks will be using your NIN for services and transactions. Imagine you walk into an Immigration office to apply for an international passport. You are asked for information verifying your identity and you just give them a number and instantly the Immigration officials connect to the National Identity Database – all your required information appears on their computer screen.

The use of biometrics according to World Bank (2015); OECD, (2007) and Oxford Internet Institute, (2007) has plenty of advantages and disadvantages regarding its use, security and other related functions. Biometrics is beneficial because they are:

- hard to fake or steal, unlike passwords;
- easy and convenient to use;
- generally, the same over the course of a user's life;
- nontransferable; and
- efficient because templates take up less storage.

Disadvantages, however, include the following:

- It is costly to get a biometric system up and running.
- If the system fails to capture all of the biometric data, it can lead to failure in identifying a user.
- Databases holding biometric data can still be hacked.
- Errors such as false rejects and false accepts can still happen.
- If a user gets injured, then a biometric authentication system may not work -- for example, if a user burns their hand, then a fingerprint scanner may not be able to identify them.

**Methodology**

Data generation technique for the study was through the content analysis of secondary data from books, journals, magazines and web resources. Concepts related to identity, identity management, interoperability and law enforcement are amply explained in order to polish their meanings for better comprehension. Hence, the study is purely exploratory and the analysis qualitatively done.

**Findings**

Information security and ensuring personal privacy are growing concerns in today’s society. Current authentication schemes use tokens and passwords but this does not really distinguish between authorized users and persons who are in the unauthorized possession of the token or password.  Using NIMC as a case, we observed that biometrics-based authentication has many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forge. We have shown that the intrinsic bit strength of a biometric signal can be quite good, especially for fingerprints, when compared to conventional passwords. Yet, any system, including a biometric system, is vulnerable when attacked by determined hackers. We have highlighted eight points of vulnerability in a generic biometric system and have discussed possible attacks. We suggested several ways to alleviate some of these security threats. To address this issue, we have proposed collaboration and publicity among government agencies among other suggestions.

Biometric authentication promises to overcome these problems but raises other concerns:

1. Biometrics is not secret: Biometrics (even fingerprints)can be recorded and misused without a user's consent.
2. Biometrics cannot be revoked or cancelled: Biometrics are permanently associated with a user.
3. A compromised biometric is forever compromised: All applications that use the biometric are compromised.
4. Cross-matching can be used to track individuals: A user can be tracked if organizations share their databases.

While biometrics presents obvious advantages over password and token based security, we presented some security and privacy concerns raised by biometric authentication. We outlined the advantages and disadvantages of biometrics and presented a case study of applying this technique to fingerprint data collection by NINC.

## Recommendations/Conclusion

In order to ensure that efforts to increase the biometrics enrollment numbers work, the NIMC has been advised to not only open up special units to deal with complaints and worries of Nigerians, but also to carry outreplace sensitization campaigns in order to convince more Nigerians on the importance of the digital identity. Such sensitization campaigns, it has been recommended, should be done even in indigenous languages.

Governors at the states should collaborate with the Federal Government. The former would serve as implementing partners to ensure efficient and effective service delivery. With the collaboration of NIMC and trained enrolment officers across the states is geared to enable them discharge their services diligently and ensure the success of the exercise. The states participation would further enhance service delivery in payroll, tax verifications, payments and scholarship awards. For instance, enrolment in schools, provision of health care services, especially through the state social health insurance scheme, among other services would be further enhanced through the NIN centre.

## References

Aliyu, A. A. (2017), *Overcoming Data Integration Challenges,* Abuja, Nigeria: National Identity Management Commission.

Anderson, C., Biscaye, P., Coney, S., Ho, E., Hutchinson, B., Neidhartdt, M., & Reynolds, T. (2016). *ICT Facts and Figures. International Telecommunications Union.*

Asian Development Bank. (2016). Identity for Development for Asian and the Pacific. Mandaluyong City, Philippines.

Ayamba, I., & Ekanem, O. (2016). *National Identity Management in Nigeria: Policy Dimensions and Implementation.* Research Gate.

Chakrabarty, N. K. (2012). UID (Aadhaar) – Its effect on financial inclusion. *The Management Accountant,47*(1), 35–3.

Chaum, D. (1985). Security without Identification, Transaction System to make big brother obsulette, *Communication of the ACM 27, (10)* Pp 1030 – 1044.

Dreze, J. (2010, November 25). Unique facility or recipe for trouble. *The Hindu.*

Drucker, P. (1988). *The Coming of the New Organisation*. Harvard Business Review, January-February.

Gallego, J. M., Gutiérrez, L. H., &. Lee, S. H., (2019). A firm-level analysis of ICT adoption in an emerging economy: evidence from the Colombian manufacturing industries. *Industrial and Corporate Change*, vol. 24, no. 1, pp. 191–221, 2014.

Gerdeman, D. (2012). India's ambitious National Identification Program. *Harvard Business School, Working Knowledge, 1–2.* Retrieved from *http://hbswk.hbs.edu/item/6957.html*

Greenwood, D. (2007). *The context for Identity Management Architectures and Trust Models.* Paper presented atthe OECD Workshop on Digital Identity Management, Trondheim.

Gobble, M. (2014). Design thinking. *Research Technology Management*, Vol. 57 No. 3, pp. 59-62.

Hansen, M., Krasemamn, H., Krause, C., Rost, M., &Genghini, R. (2003). Identity Management Systems (IMS). *Public Administration Research Vol. 9,* No. 1; 2020

Hickson, D.J., Hinings,C.R., Lee, C.A., Schneck,R.E., and J.M. Pennings (1971). A strategic contingencies theory of intraorganizational power. *Administrative Science Quarterly*, Vol. 16 (2): 216 – 229. DOI 10.2307/2391831.

Hilbert, M., & López, P. (2011). The world's technological capacity to store and communicate. *Computer Information Science*, vol. 332, no. 6025, pp. 60–65.

Identification and Comparison (2012). Technical Report, Independent Centre for Privacy Protection (ICPP), Kiel(Germany). Study made for the Institute for Prospective Technological Studies – Joint Research CentreSeville (Spain). Retrieved September 27, 2012, from *http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS_Study.pdf*

Kant, C., & Sharma, Y. (2013). Enhanced Security Architecture for Cloud Data Security. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 570-575.

Kaushik, M. (2010). Configuring the UID. *Business Today, 19*(22), 12.

Kohntopp, M. (2001). Collection of Information on IdentityManagement and link list (Partly in German and partly in English *http://www.Koehntopp.de/marit/pub/idmanage/.*

Liberty Alliance Project. (2004). Whitepaper: Benefits of Federated Identity to Government.

Lips, M., & Pang, C. (2008). *Identity Management in Information Age Government Exploring Concepts, Definitions, Approaches and Solutions*. Victoria University of Wellington, Kelburn, New Zealand.

Malik, T. (2014). *Technology in the Service of Development: The NADRA Story.* Retrieved from

http://www.cgdev.org/publication/technology-servicedevelopment

Mukherjee, A., & Nayar, L. (2011, December 5). *Aadhar-A few basic issues.* Outlook India.

Musa, Y. (2000, October 13). Nigeria: ID Cards May Control Rigging. *Weekly Trust*, pp. 10.

National Identity Management Commission. (2013). *Harmonization and Integration Policy.* Retrieved May 7, 2016. *www.nimc.gov.ng*

National Identity: NIMC captured 14 million Nigerians by 2016. (2017, February 17). *Technology Time*. https://doi.org/10.1016/S1350-4789(16)30303-8

National ID-NIMC 'captured 14 million Nigerians' by 2016. (2017, February). *Big Story.* Retrieved fromtechnology times.ng/nimc-captures-14-million-Nigerians-national-id

O'Brien, J.A. (1996) *Management Information Systems* ,USA: McGraw Hill

OECD(2007). *OECD Recommendation on Electronic Authentication and OECD Guidelines for Electronic Authentication.* Retrieved from www.oecd.org/dataoecd/32/45/38921342.pdf

OECD. (2011). *National Strategies and Policies for Digital Identity Management in OECD Countries.* OECD Digital Economy Papers, No. 177.

Organisation for Economic Cooperation Development Report. (2011). *Digital Identity Management*: Enabling Innovation and Trust in the Internet Economy.

Oxford Internet Institute. (2007). *E-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector*: Oxford Internet Institute.

Pati, R. K., Kumar, V., & Jain, N. (2015). Analysis of Aadhaar: A Project Management Perspective. *IIMKozhikode Society & Management Review, 4*(2), 124–135.

Peshwani, P., & Joshi, B. (2016, October 26). *Aadhaar – Identification Simplified, Myths Busted.* The Wire.

Ramanathan, U. (2010). The personal is personal. *The Indian Express*, *International Environmental LawResearch Centre.* Retrieved from http://www.ielrc.org/content/n1002.Pdf.

Udunze, B. (2014). $55m biometric budget: CBN, NIMC at war over control of BVN scheme. The Sun Retrieved from *http://sunnewsonline.com/new/55m-biometricbudget-cbn-nimc-atwar-over-control-of-bvn-scheme/*

World Bank (2015). Identification for Development: Nigeria. Conference Report. (2015). Washington. Retrieved from *https://openknowledge.worldbank.org/handle/10986/26437*

Oluwadare, A. O. (2020). An Administration of the New Electronic Identity Management System in Southwestern Nigeria. *Public Administration Research; Vol. 9,* No. 1; Pp. 1-9.