International Journal of Management and Humanities (IJMH)
ISSN: 2394-0913 (Online), Volume-8 Issue-10, June 2022

Critical Analysis of the Vulnerabilities Surrounding the Use of Pos Services in Rural Communities in Nigeria

Fergus Uchenna Onu, Ikechukwu Jonathan Ezea

Abstract: ***In a bid to implement the policy of financial inclusion for both urban and rural dwellers in Nigeria, the Point-of-Sale (POS) services has been deployed for financial transactions in the rural communities of the country. This paper took a critical study of the operations of the POS services in rural Nigerian communities-rayed the opportunities it created, analyzed the vulnerabilities surrounding the service and suggested ways of protecting the stakeholders (customers and agents) using the POS services. The paper has done all these to enlighten the POS customers in order to keep their funds safe and also build a trust in the system and thereby helps to achieve the expected financial inclusion.***

Key words: ***Vulnerability, POS Services, rural communities, financial inclusion***

I. INTRODUCTION

The advent of the liberalization of the telecommunication industry in Nigeria in 1999 opened a lot of business opportunities in many facets of the economy both in urban and rural communities. One of such opportunities is the use of Point of Sale (POS) machines in businesses and financial transaction. The POS although has been in use since 1879 in manual form. It has undergone reformation from manual to electric in early 1900 and in the past two decades it has gone into mobile connection. In 2013, the Central Bank of Nigeria (CBN), in a way to implement its policy of financial inclusion and cashless economy in Nigeria gave credence to the use of POS as an agent tool for agency banking (CBN, 2011) This has made the use of POS in Nigeria very popular for the past ten years. Presently. There are about 542,109 POS terminals in Nigeria as at December 2021(*Doris, 2022*). As the POS increases, the vulnerability and management also increases. According to Ford (2018 et al) Vulnerability denotes susceptibility to harm and is derived from the Latin word *vulnerate*, meaning "to wound. It is a state of being likely to be hurt. Vulnerability is a growing concern for individuals, political leaders, and academics (Misztal, 2012; Oris et al., 2016; Ranci, 2010).

Manuscript received on 30 May 2022.
Revised Manuscript received on 02 June 2022.
Manuscript published on 30 June 2022.
* Correspondence Author
Fergus Uchenna Onu, Department of Computer Science, Ebonyi State University, Abakaliki Nigeria. E-mail: uche.fergus@gmail.com, fergus.onu@ebsu.edu.ng
Ikechukwu Jonathan Ezea*, Department of Computer Science, Ebonyi State University, Abakaliki Nigeria. E-mail: iykeezea@gmail.com

Vulnerability in POS simply refers to those things, (actions and inactions) which make the use of POS unsafe or more susceptible to be unsafe for use. This simply points to customers safety while using POS machines across the Nigeria. In this financial inclusion drive, there have been many agents of the banks which are using these POS machines as tools for transactions. The big question still remains how safe are customers while using the POS machines? The rural dwellers in Nigeria are mostly peasant farmers whose livelihood depends on the sales from their cash crops. The average cash is always very small, and any loss of the smallest kobo means very much to them. Some also depend on their children who live in the cities for livelihood. The means that any loss of money through any form of epayment systems means a lot for them. This will discourage them and also affect the trust index both on the system and operators

II. TYPES OF POS MACHINES AND SERVICES THEY RENDER

Within the past two decades, three types of POS machines have been so commonly used. These are :

i. Mobile POS

This is the POS terminals that run on smartphones. For it to work, a card reader is attached where the user can conveniently insert the card reader for transactions.

ii. Desktop POS

This type of POS works on computer or laptop either as a desktop application or an application. This type of POS is best used in retail stores that have cash dedicated cash wraps where cashiers ring up sales.

iii. Multifunction POS

This is our regular POS that is very common in Nigeria. This type of POS can be attached to the computer system or other mobile devices. It is such a flexible device that can be used in shops, event and any type of environment.

III. ANALYSIS OF VULNERABILITIES IN POS.

The vulnerabilities in POS machine operations can be classified into two main types depending on what influenced it.

A. Internal Vulnerability

Internal vulnerability simply means the situation in which the use of POS is vulnerable due to an insider act. This insider vulnerability is divided into two: the agents/operators and the bank relationship personnel.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

i. This agent or operator.

The agent or operator is the merchant in whose custody is the POS machine. In our local communities, he or she operates it for the customer due to the level of literacy. Internal vulnerability is very dangerous since customers rely mostly on the agent or operator's integrity to use the POS. Today operators get POS without any screening by any known body except the bank confirming that he/she is a customer and has been doing business with the bank for some time. This has proved to be the worst part of the vulnerability as the operator capitalizes on the literacy levels on the local communities who even voluntarily give their ATM cards and Personal Identification Number (PIN) to the operators to operate for them. In July 2021, according to Premium Times Newspaper, customers were defrauded over 900 million naira between January and May 2021.

ii. Bank Relationship Personnel

This is another category of the insider vulnerability. When fake POS machines and deployed to fake agents by bank personnel. According Premium Times March 11, 2021 reported that some POS machines are now being deployed by scammers. The new POS, according to the source, can store customers' information even after transactions are carried out and the card removed. The POS can retain the information for future use to defraud the original owners of the ATM card. This fake deployment is done by fraudulent bank personnel with fake operators. Our local communities do not know which is which and fall victim of these people.

iii. The Customer

Nigeria has a population of 48.08% people in rural areas. It is also clear that majority of this rural people are illiterate. According to National Commission for Mass Literacy (2020) report, 35% of the adult in Nigeria are illiterate. This makes them vulnerable in the use of all digital platforms. Our rural communities are vulnerable due to illiteracy. Most of them drop their ATM cards and their PIN to the agents or operators who capitalize on their illiteracy and trust on them to defraud them. This makes the use of POS machines vulnerable.

B. External Vulnerability

External vulnerability is a situation where an intruder interferes with the operations of the POS machines. Today, the POS is connected to all kinds of network for connectivity. This connection makes it vulnerable as hackers can interfere with the connection. External vulnerability also includes those kinds of chip installation in the card readers on POS by external person without the knowledge of the operator or agent who may not even know what the attacker wanted to do. These chips are inserted into the card reader and normally picks the 16 digits of the ATM card of the customer and also captures the password. These attackers get connected to the POS machine and usually use these details for online transfers and other online transactions. These attackers made the POS vulnerable to several other weaknesses and make the use unsafe.

C. The Design Vulnerability

Today, transactions in POS machines by design are still authenticated through a single authentication method. A single factor is not reliable to provide adequate protection due to a number of security threats. Authentication remains a fundamental safeguard against illegitimate access to the device or any other sensitive application, whether offline or online, (Boyd, 2013). The Single Factor Authentication (SFA) as the name implies is the application of only one authentication method to gain access to a channel. This type of authentication is the oldest and simplest methods. Using the SFA simply matches ones credentials and validates it to give such user access to the platform. Single-factor approach is based on a "what you know" (Nancie, 2010). As an example, the use of a password (or a PIN) to confirm the ownership of the user ID could be considered. Apparently, this is the weakest level of authentication according to (Dasgupta et al, 2016) and (Bonneau et al, 2015). This is what is obtainable in POS machine as the only authentication method.

IV. CHALLENGES THAT LEAD TO VULNERABILITY

There are challenges of using POS in our rural communities today that make POS service vulnerable. They include

1. Customer and operator literacy level
2. Customers unaware of cybersecurity issues
3. Poor network connectivity that can lead to denial of service
4. Fear and change resistance.
5. Scammers posing as agents.
6. Help me cash money (middleman); customers sending

V. WAYS OF MITIGATING POS VULNERABILITIES

Having reviewed the critical vulnerabilities in POS, the following are the suggested ways to mitigate, eradicate or at least reduce the vulnerabilities to the barest minimum

1. Operators and agents must ensure that all POS are connected to a secure network to avoid hacking and man in the middle activities.
2. There should be regular update of all POS machines with patches and security updates to ensure the POS is secure and a lock out should be implemented as a policy that any POS that is not updated should not be able to connect to the network.
3. Banks should do an integrity test on all agent and operators of POS and ensure that they are genuine and reliable operators.
4. An awareness should be created for all customers, so they don't share or expose their PINS.
5. Operators and agents must be follow best practices.
6. POS transaction involves cash and confidential information is involved, there is the need that agents and operators must do so in secure environment to avoid physical interference that will expose the details of customers or make the machines exposed to bad people.
7. Investigate the source of the POS terminal to confirm that it is genuine.
8. create awareness for operators and customers in rural areas.

VI. CONCLUSION

Most rural areas today do not have banks and even where banks exist, the rural dwellers prefer to use the POS because it is faster and less cumbersome to use to collect cash. It is unarguable that there are various opportunities in using POS which ranges from easy access, asses and even familiarity with most local operators as highlighted in the body, however there are challenges which include the internal and external vulnerabilities. Ways to overcome these internal and external vulnerabilities have also been dealt with. It is also recommended that an improved authentication method is added into the POS machines used in rural areas in Nigeria POS is the surest way to financial inclusion considering that most of our rural communities do not have access to traditional banks. It is very necessary that both the actors and regulators should take a deep dive into the services of POS to be able to make it vulnerability free. This can be achieved through multilevel of authentication considering that any money lost by the rural dwellers means a lot to them.

REFERENCES

1. Boyd, C.; Mathuria, A. Protocols for Authentication and Key Establishment; Springer: Berlin, Germany, 2013.
2. CBN (2011), ''Guideline for Point of Sale (POS) card acceptance services in Nigeria'' http://www.cenbank.org/POS/asp.
3. Doris Dokua Sasu :Number of POS terminals in Nigeria 2017-2021, Published by Statisca, Feb 1, 2022
4. Ford, J.D., Pearce, T., McDowell, G. et al. Vulnerability and its discontents: the past, present, and future of climate change vulnerability research. Climatic Change 151, 189–203 (2018). https://doi.org/10.1007/s10584-018-2304-1 [CrossRef]
5. Misztal, B. A. (2012). The challenges of vulnerability. London, England: Palgrave Macmillan [CrossRef]
6. Premium Times Nigeria: EFCC arraigns four for N900 million POS fraud,12thJuly 2021,
7. Ranci, C. (2010). Social vulnerability in Europe. In C. Ranci (Ed.), Social vulnerability in Europe. The new configuration of social risks (pp. 3–24). London, England: Palgrave Macmillan [CrossRef]

AUTHORS' PROFILE

Fergus Uchenna Onu, has a PhD in Computer Science. A Senior Lecturer with Ebonyi State University, Abakaliki. A Fellow of the Nigeria Computer Society (NCS), the Immediate past Director of ICT/Research Center in Ebonyi State University. He is an ardent researcher in the areas of Computer and data communications, Software and applications development and programming languages.

Ikechukwu Jonathan Ezea, is currently the Country Head Technology & Services, FBNBank Sierra Leone, a subsidiary of First Bank Nigeria Ltd. Prior to his secondment to the subsidiary, he was the Head of ATM/POS Channel Support, First Bank of Nigeria Ltd. He holds MSc. in Information Technology. He is a member Nigeria Computer Society and a Fellow Institute of Information Managers Africa (IIMA). He is presently a Post graduate student at Ebonyi state University Abakaliki. His research interest is in data communication and network and application security of banking applications.