Challenges of Cyber Security Platforms in Nigeria: Empirical Analysis and the Way Forward

Uzukwu, Joy Ebere
Ph.D. Student, Department of Information Technology,
Federal University of Technology, Owerri, Nigeria

Nworuh, Godwin
Lecturer Department of Information Technology,
Federal University of Technology, Owerri, Nigeria

Asiegbu, Baldwin, Chukwunanu
Lecturer Department of Information Technology,
Federal University of Technology, Owerri, Nigeria

Ahaiwe, Josiah
Lecturer Department of Information Technology,
Federal University of Technology, Owerri, Nigeria

Nwokorie, Chioma, Euphemia
Head, Department of Computer Science Department,
Federal University of Technology, Owerri, Nigeria

Abstract
Cyber security challenges have become prevalent in Nigerian banking system even as crude oil prices continue to fluctuate. The present platforms are unable to adequately meet up with the incessant occurrences of cyber threats. Sequel to this, the research identified performance indicators of the system under study and evaluated the performance for e-payment fraud controls. Field survey was carried out on the present platforms. Their performance was validated in relation to the identified performance indicators and Z-test served as the analytical tool. A null hypothesis was studied. From the analysis of hypothesis, the probability value (0.017) is less than the alpha value (0.05), the researcher therefore rejected the null hypothesis and concluded that the present security strategy has a significant challenge in providing security in e-payment transactions. The work is of the opinion that for Nigerian banking system to combat these security challenges, there is a need to integrate several competent cyber security platforms such as the integrated system using Layer 8 Human Identity Firewall, SHA-3 cryptographic algorithm, Intrusion Detection Prevention System coupled with a “honey pot” to provide a better security measure.

Keywords: Performance indicators, cyber security, platforms, firewall, challenges, cryptography

1. Introduction
The Information Technology industry has gone from the widespread use of ATMs in the 1980s, to modern point of sale (PoS) terminals in the 1990s, to internet banking in the 2000s and mobile banking in 2010s. These new ways of meeting customer’s demand, however, come with new fraud patterns and evolving risks of ATM fraud and phishing attacks in e-payment. Among the common risks in the banking sector are Automated Teller Machine (ATM Cash Out) attacks and Corporate Account Take Over / e-payment attacks, especially through phishing, (DCFS, 2014). These are what firewall and cryptography attempt to provide a solution to in this research.

Electronic fraudsters had invaded Nigerian banking environment, deploying over 185 fake mobile applications on the websites of 15 out of 17 deposit money banks with which they are extracting customers’ personal and financial information with intent to steal billions of naira from bank accounts, (APWG, 2015). Also DCFS (2015) notes that phishing and insider threats will continue to be the biggest cyber threat sources in Nigeria, especially as crude oil prices continue to fall. NIBSS (2015) reveals that there was 85 percent success in fraud attempts. It also notes that automated teller machines (ATMs) had most fraudulent transactions while Internet banking fraud loss was put at N3.2 billion within the last three years. NIBSS (2014) equally indicates that 1,461 cases of electronic fraud were recorded in that year, which was a significant increase from the previous year’s figure. Suleiman (2014) notes that the Central Bank of Nigeria presently has certain measures going on, helping to curb the fraud, though they are still inadequate since the incidence remains alarming. Some of the measures are the following:
Mandating all organizations (financial) to comply with the provisions of section 3.2 and 3.4 of the Standards and Guidelines of ATM Operations in Nigeria by installing anti-skimming devices on their ATMs.

Providing a policy that restricts banks from approving international card and transactions unless the customer has informed his or her bank.

Issuing of the two-factor authentication implementation directive for internal banking processes in all banks.

Certifications such as Payment Card Industry Data Security Standard (PCI DSS). For banks.

The review of operations of instant payments system within the country.

Partnering in order to procure and install an industry anti-fraud solution.

Directing all stakeholders to establish and maintain dedicated Fraud Desks in their respective organizations.

Calling on banks to create a secured environment, deploy brand anti-fraud intelligence as well as safe browsing and device analytics.

Instructing the banks to have a forum to equip themselves with information and technologies to be a step ahead of cybercriminals.

2. Research Question
To what extent does the existing system perform in relation to the identified performance indicators?

2.1. Hypothesis
The null hypotheses for this work is:

- The present security strategy has no significant challenge in providing security in e-payment transactions.
  - Which is tested against the alternative hypothesis:
- The present security strategy has significant challenges in providing security in e-payment transactions.

2.2. Performance Indicators of the Existing Cyber Security Platforms
Villegas (2016) notes the following performance indicators for cyber security systems:

- Daily periodic security monitoring results
- Security embedded into new technology or system tools and services
- Reduction in false positives
- Increase in customer satisfaction
- State of security executive management reports
- Attack detection

NIBSS (2014) provides a statistics on the rate and nature of fraud in e-payment and ATM transactions in the banking system. It notes that globally, fraud is on the rise as well as its sophistication. Fraud in the Nigerian payments system and also on a global scale has been on the increase over the past few years as technological advances impact on the way we pay. Internet banking, the ever increasing use of the ATMs and other electronic platforms has one way or the other accelerated the growth of fraudulent activities. Cheques and over-the-counter fraud has given more room to a sophisticated and more concise electronic type of fraud. In Nigeria, Internet banking and ATM scored as the lead channels for perpetuating e-fraud in 2014 as it recorded the highest value lost to fraudulent activities (NIBSS, 2014).

The CBN guidance on electronic banking states that “banks must take additional steps to ensure that whilst the web ensures global access to data enabling real time connectivity to the bank’s back-end systems, adequate measures must be in place to identify and authenticate authorized users while limiting access to data as defined by the Access Control List”. Banks are required to ensure that unnecessary services and ports are disabled. In line with the CBN guidance on “Standards on Protocol”, banks adopt the current and reliable security measures to authenticate and protect customers’ information while transacting on the websites (Weinsberg, Tzur-David, Dolev, and Anker, 2016).

While the Internet is generally an unsecure network, it may be made secure through the implementation of process controls and infrastructure components (Stakhanova, Basu and Wong, 2007). CBN recommend a minimum of two-factor authentication process for all user access to the services provided which could be high-risk transactions involving access to customer information or the movement of funds to other parties (Weinsberg, Tzur-David, Dolev, and Anker, 2016). Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks (Weinsberg, Tzur-David, Dolev, and Anker, 2016). In a study by Salah and Kahtani (2010), it was discovered that two modes of encryption are in use among Nigerian commercial banks; they are 128bit and 256bit Secure Socket Layer (SSL). While some banks, such as Zenith, GTB, Oceanic and some others uses the 128-bit SSL, few others such as Skye bank and Standard Chartered uses 256bit SSL. This can be recognised at the address bar which starts with ‘https’. Also, a padlock symbol will be noticed at the bottom of the browser (Stakhanova, Basu and Wong, 2007). This encryption technology ensures that data passing between customer computer and the bank is secure and that customer accounts cannot be accessed by anyone else online (Dutkevych, Piskozub and Tymoshyk, 2007).
3. Some Existing Cyber Security Platforms and their Challenges

3.1. Intrusion Detection System

Nong (2002) notes that an Intrusion Detection System is a defense system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers). An intrusion happens when somebody (hacker or cracker) attempts to break into or misuse your system while misuse is broad, and can reflect something severe such as stealing confidential data or something minor such as misusing email system for spam. Hence, Intrusion Detection System (IDS) is a software or hardware product that monitors the events occurring in a computer system or network and analyses them for signs of intrusions while Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity. Suchita and Meshram (2012) note the following disadvantages of IDS:

The disadvantages are:
- It can deny legitimate access in false alarm scenarios.
- It is difficult to apply new signatures without sensor reboot.
- IDS sensor response actions cannot stop the trigger packet and are not guaranteed to stop a connection. IDS response actions are typically better at stopping an attacker more than a specific attack itself.
- IDS sensor response actions are less helpful in stopping email viruses and automated attackers such as worms.
- Users deploying IDS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IDS deployments. Users must spend time to correctly tune IDS sensors to achieve expected levels of intrusion detection.
- Being out of band (OOB), IDS sensors are more vulnerable to network evasion techniques, which are the process of totally concealing an attack.

3.2. Intrusion Prevention System

Deris, Ala’ Yaseen, Mohd, Kamarulnizam and Abdul (2012) note that Intrusion Prevention System (IPS) is primarily a network-based defense system, with increasing global network connectivity. It combines the technique of firewall with that of the IDS properly with proactive technique. This system is a proactive technique which prevents attacks before entering the network by examining various data record and detects demeanor pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs the offending data. Suchita and Meshram (2012) states that Intrusion Prevention Systems technologies are differentiated from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. The key to differentiating IDS from IPS is that an IDS responds immediately and does not allow any malicious traffic to pass, whereas an IDS allows malicious traffic to pass before it can respond. According to Ido, Tzvi, Moshe (2007) and Suresh, Charli, and Pau-Chen (2003), there are many flavors of IPS, but the basic function of each is to detect and stop attacks by either dropping sessions, resetting sessions, blocking packets, or proxying traffic. An IPS can be either hardware, software, or a combination hardware/software solution. The five main types of Intrusion Prevention System are in-line detection, layer seven switches, deceptive systems, application firewalls, and hybrid switches.

Computer system security has become a major concern over the past few years. Attack, threat or intrusions against computer system and network have become commonplace events, many system device and other tools are available to help counter the threat of these attacks. Guillen, Padilla and Colorado (2009) and Cao, Zhihong, Tie, Zhonde and Jiren (2009) highlight current countermeasure against security violation such as (i) firewall which strengthen the implementation of executing rules and policy, but firewall can do nothing about attack from inside network and cannot clarify behavior or anomaly attack, (ii) antivirus software which unfortunately has very limited ability to pattern recognition of new viruses (iii) Intrusion Detection which only send the alert to trigger after attack have entered the network, and do nothing to stop attacks.

Currently, IDS technologies are not very effective against predicting a new mechanism of attack. There are several limitations, such as performance, flexibility, and scalability. Intrusion Prevention System (IPS) is a new approach to defense networking systems, which combine the technique of firewall with that of the Intrusion Detection properly, which is a proactive technique and prevents the attacks from entering the network by examining various data records and detecting demeanor of pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs the offending data. Recently, intrusion detection systems are used to manage traffic in real-traffic for increasing the accuracy of detection and decreasing false alarm rate. In some instances, IPS adopts techniques from intrusion detection, such as detection approach, monitoring sensor, and alert mechanism (Ghorbani, 2009).

Fuchsberger (2005) describes the fundamentals of IDS and IPS and notes that currently, IDS can be seen as a traditional second line of defense system. It is becoming more difficult to apply security access control on it. On the contrary, IPS can be used to alarm for attacks within a network and provide for action on attack prevention with Firewall and IDS function mechanism. Performed work in Ollmann (2003) outlines the future trends of IPS in its functionality such as: gateway appliance, perimeter defense appliance, all-in-all capability, and network packet inspection/prevention.
An IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time (Ghorbani, 2009). IPS combines the technique firewall (data link layer, network layer, transport layer and application layer) with that of the IDS properly with proactive technique, it is a new approach system to defense networking systems and prevents attacks from entering the network by examining various data record and prevents demeanor in pattern recognition sensors. When an attack is identified, intrusion prevention blocks and logs the offending data.

Suchita (2012) notes some common characteristics of IDS and IPS technologies: IDS and IPS technologies are deployed as sensors. An IDS or an IPS sensor can be any of the following devices: a router configured with IPS software, an appliance specifically designed to provide dedicated IDS or IPS services, a network module installed in an adaptive security appliance, switch, or router. IDS and IPS technologies typically monitor for malicious activities in two spots:

- Malicious activity is monitored at the network to detect attacks against a network, including attacks against hosts and devices, using network IDS and network IPS.
- Malicious activity is monitored on a host to detect attacks that are launched from or on target machines, using Host Intrusion Prevention System (HIPS). Host-based attacks are detected by reading security event logs, checking for changes to critical system files, and checking system registries for malicious entries.

IPSs expanded on the functionality provided by IDS by enabling to prevent attack against of network. Dutkevych, Piskozub and Tymoshyk (2007) present real-time intrusion prevention and anomaly system and notes that the main problem of IPSs is that they can effectively detect only the attack they know from signature.

In the same vein, Schultz, et.al. (2007) note the disadvantages of IPS technology, such as the following:

- An IPS sensor will affect network timing because of latency, jitter, and so on. An IPS sensor must be appropriately sized and implemented so that time sensitive applications, such as VoIP, are not negatively affected.
- An IPS sensor must be online and, therefore, IPS sensor errors or failure can have a negative effect on network traffic.
- Overrunning IPS sensor capabilities with too much traffic does negatively affect the performance of the network.
- Users deploying IPS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IPS deployments.

3.3. Layer 7 Firewalls

Layer 7 firewall (application firewall) is a form of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. The application firewall is typically built to control all network traffic on any OSI layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is without additional software, unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls (Jeremy, 2006).

3.4. SHA-1 (Secure Hash Algorithm 1)

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States (Stevens, Bursztein, Karpman, Albertini and Markov, 2017). It produces a 160-bit (20-byte) hash value known as a message digest and an SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. SHA-1 produces a fixed-length hash value of 160 bits, or 40 hexadecimal characters and it is is able to process only input data with a maximum length of (2^64 – 1) bits. The algorithm is based on the MD4 and MD5 hashing algorithms. SHA-1 produces a larger hash value (160 bits) than MD5 (128 bits), thus making it harder to crack with brute force or reverse engineering even though the computation time for this longer hash value makes SHA-1 slower than MD5.

It is notable that SHA-1 is no longer considered secure against well-funded opponents because in 2005, cryptanalysts found attacks on SHA-1 suggesting that it might not be secure enough for ongoing use. Therefore since 2010, many organizations have recommended its replacement by SHA-2 or SHA-3. Stevens (2012) notes that the following list describes the disadvantages of SHA-1.

- SHA-1 is so weak to newly refined attack that it may be broken by real world hackers.
- It has been marked as unsafe in modern internet browsers.
- It is not vastly more difficult to create a document that matches a given hash than it is to create a hash from a given document.
- Is a slower computational algorithm than the MD5 algorithm
- Has known security vulnerabilities

3.5. SHA-2 (Secure Hash Algorithm 2)

SHA-2 is a set of cryptographic hash functions designed by the United States National Security Agency. Cryptographic hash functions are mathematical operations run on digital data by comparing the computed “hash” (the output from execution of the algorithm) to a known and expected hash value. A person can determine the data integrity. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with. A key aspect of cryptographic hash function is their
collision resistance, nobody should be able to find two different inputs values that results in the same hash output (NIST, 2012).

In 2005, an algorithm emerged for finding SHA-1 collisions in about 2000-times fewer steps than was previously thought possible. The security margin left by SHA-1 is weaker than intended, and its use is therefore no longer recommended for applications that depend on collision resistance, such as digital signatures. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2 (NIST, 2012). However, the NIST hash function competition selected a new hash function, SHA-3, in 2012 (Eichlseder, Mendel and Schläffer, 2014).

Mendel, Nad and Schläffer (2013) note the following disadvantages of SHA-2:

- The weaknesses in collision resistance that have been identified make the algorithm vulnerable to possible exploitation over the coming years.
- The use of SHA-2 on websites may pose a problem if the end user has an older operating system.

Existing platforms lack the necessary features to combat cyber security. Domke (2014) notes that weaknesses have been reported in SHA-1. It is so weak to newly refined attack that it may be broken by real world hackers. Also, it has been marked as unsafe in modern internet browsers and it is not vastly more difficult to create a document that matches a given hash than it is to create a hash from a given document.

Popeskic (2016) notes that the use of layers 1 to 7 alone without the user layer is such that configuration cannot be set for each user ID. This makes it possible for unauthorized users to access the system. Hence, the shortcomings of Firewall without IDS and IPS are such that dynamic configuration of network is difficult and the network is not fully water tight and unhackable.

Suleiman (2014) notes that the Central Bank of Nigeria presently has certain measures going on, helping to curb the fraud, such as mandating banks to deploy a proxy type firewall. They are still inadequate since the incidence remains alarming. Nigerian banks have lost a total of N199 billion to e-fraud between 2000 and 2014, mostly due to inappropriate and reckless management of customer’s data. Globally, e-mail fraud had led to 100 billion spams per day, $2 billion in phishing losses/year while good attacks are 45 percent effective. The losses to the financial system include brand erosion, untrusted e-mail channel and lack of e-mail visibility (APWG, 2014). The source also notes that fraud cases in the nation’s financial services industry grew by 183 percent as total number of reported cases increased from a total of 3,786 in 2013 to 10,612 in the last financial year. Similarly, the amount involved in frauds increased from N21.80 billion to N25.61 billion indicating a 17.5 percent increase with expected loss rising from N5.76 billion in 2013 to N6.19 billion in 2014. The types and nature of frauds and forgeries were largely web-based online banking and ATM card related, fraudulent transfers and withdrawals amongst others. In the same vein, online transactions in Nigeria between 2012 and 2014 showed that actual loss from point of sales (PoS) increased from N5.8 million to N157.6 million, ATM increased from N55 million to N2.7 billion in 2014 while mobile banking losses increased from N6.6 million in 2013 to N13.3 million (APWG, 2014)

El-Safi (2013) proposes the use of Secure Hash Algorithm 1 for data encryption and decryption while Nwoagu (2014) and Faisal (2016) propose the use of Advanced Encryption Standard (AES) which is a SKC having 256 bits. However, Jinkeon, Kitae, Jaechal, Seokchie and Kyungho (2013) have proved it to be a weak cipher. Schneier (2015) notes that attacks have been reported on SHA-1 hence it is no more secure while there are theoretical attacks on SHA-2. Notably, Lawal, Ibitalo and Longe (2013) note that two types of encryption are in use among Nigerian commercial banks, they are 128bit and 256bit SSL. While some banks, such as Zenith, GTB, Oceanic and some others use the 128-bit SSL, few others such as Skye bank and Standard Chartered uses 256bit SSL. This can be recognised at the address bar which starts with ‘https’. Also, a padlock symbol will be noticed at the bottom of the browser (Lawal, Ibitalo and Longe, 2013).

Also Babatunde, et.al (2002) proposes the use of an Intrusion Detection System with a firewall but notes that an IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than proactive agent. It plays the role of an informant rather than a police officer. Suchita and Meshram (2012) note that IDS sensor response actions cannot stop the trigger packet and are not guaranteed to stop a connection. IDS response actions are typically better at stopping an attacker more than a specific attack itself, IDS sensor response actions are less helpful in stopping email viruses and automated attackers such as worms. Users deploying IDS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IDS deployments. Users must spend time to correctly tune IDS sensors to achieve expected levels of intrusion detection. IDS sensors are more vulnerable to network evasion techniques, which are the process of totally concealing an attack.

Byido and Tzvirir (2007) note that IDS sensor response actions are less helpful in stopping email viruses and automated attackers such as worms. Users deploying IDS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IDS deployments. Users must spend time to correctly tune IDS sensors to achieve expected levels of intrusion detection. Faisal (2016) also proposes the use of proxies which are application layer firewalls but my proposal includes the use of layer 8 firewall in addition. Popeskic (2016) however notes that there is a big issue with application firewall and that is throughput limitation. They can also full up a lot of disk space by writing many logs. The downside is a security weakness that enables the attacker to take the ownership of a non-secure device and from there attack every machine in the local network. Another thing is that the application layer firewall does not support all applications that exist today. What then is the way forward?

4. Methodology and Methods

Survey research method was used. This generally involves a large audience to collect a large amount of data. This is a quantitative method having a predetermined set of closed questions which are pretty easy to answer. Because of the
simplicity of such a method, high responses are achieved. It is one of the most commonly used methods for all kinds of research in today’s world. This method involves collecting a large amount of data from a large population, most usually by questionnaires or structured interviews. Most usually it is a quantitative method, involving ‘closed’ questions with a predetermined number of answers. These are in fact much easier to fill in and therefore more likely to get a high response rate, as does keeping the questionnaire short. The tool for the analysis and validation of the work is Z-test. Two types of data were used: the primary and the secondary data. Data was collected by means of interviews and questionnaire, secondary data collection and research through the internet. The information obtained from the interview and questionnaire provided primary research data that supported the study. The secondary data on the other hand, were derived from the findings stated in published documents and literatures related to the research problem.

5. Methods of Data Collection and Characteristics of the Population

The population is the users of the existing system of data traffic control in Nigerian banks. These are the Information Technology staff in banks. 11025 Information Technology personnel are used as the population of the study. They are the users of the new system of data traffic control. They are subjects to the 21 money deposit banks in Nigeria. Banking system in Nigeria is regulated through the apex bank, the Central Bank of Nigeria. It has a subsidiary, Nigeria Electronic Fraud Forum (NeFF) which consists of all relevant stakeholders to actively and proactively react to this challenge to safeguard integrity of the e-payment channels. The Nigerian Deposit Insurance Corporation (NDIC) complements the regulatory and supervisory role of the CBN. It is however autonomous of the CBN and reports to Federal Ministry of Finance. Also The Nigerian Inter Bank Settlement System (NIBSS) is autonomous and complements the functions of the Central Bank of Nigeria.

6. Reliability Test

The Cronbach alpha coefficient gives a measure of the accuracy or consistency with which a set of items measure a single construct. Decision guidelines for interpretation of the Cronbach coefficient was: < 0.60 unacceptable, 0.60-0.65 undesirable, 0.66-0.70 acceptable (which connotes a fair degree of internal reliability), 0.71 - 0.80 respectable (which connotes a good degree of internal reliability), 0.81 - 0.90 very good (which connotes a very good degree of internal reliability), and > 0.90 (which connotes a very high/good degree of internal reliability).

To ensure that the instrument will be able to elicit consistent result, it was tested for internal consistency using Cronbach’s Alpha test. The pilot study was conducted using twenty five percent (25%) of the sample size of the study which is ninety five (95) copies of questionnaire. At the end, seventy nine (79) copies were retrieved representing twenty one percent (21%) of the sample size. The result obtained is shown in the table below:

| Case Processing Summary |         |     |
|-------------------------|---------|-----|
| Valid                   | 79      | 100.0 |
| Cases Excluded          | 0       | 0.0 |
| Total                   | 79      | 100.0 |

Table 1: Case Processing Summary

\[ a. \] Listwise deletion based on all variables in the procedure

| Reliability Statistics |         |
|------------------------|---------|
| Cronbach’s Alpha       | 0.883   |
| Cronbach’s Alpha Based on N of Items | 0.889     |
| Standardized Items     | 79      |

Table 2: Reliability Statistics

Sources: SPSS output. Ver. 23

From the result obtained, the reliability coefficient was .889 which if converted into percentage is 88%. This signifies that the instrument is reliable and capable of eliciting consistent result.

7. Sampling Procedure

The sample size was obtained through the use of Yaro Yamane formula for determining the sample size. This is given by:

\[ n = \frac{N}{1 + N(e^2)} \]

Where: \( n \) = sample size.
\( N \) = population of interest, which is 11,025.
\( e \) = error estimate/level of significance, which is normally 5%

Solving:

\[ n = \frac{11025}{1 + 11025(0.05)^2} \]
\[ n = 386 \]
Since the sample size is already determined (386), the sample size for each bank is further determined by calculating its proportion to the population. Simple random sampling was used in the final stage of selecting the sample of study from the list of the number of staff in the twenty one banks of study. The relevant formula goes thus:

\[ ns = \frac{N_p \times n}{N} \]

- \( ns \) = the sample size allocated to each unit
- \( N_p \) = the population size of each unit
- \( n \) = the total sample size
- \( N \) = the total population size

The resulting sample allocations are presented in table 3 below.

| Banks | Population | Sample |
|-------|------------|--------|
| 1     | Access Bank | 778    | 27     |
| 2     | Citibank    | 329    | 12     |
| 3     | Diamond Bank| 701    | 24     |
| 4     | Ecobank     | 541    | 19     |
| 5     | Fidelity bank| 726   | 25     |
| 6     | First Bank of Nigeria | 732 | 26     |
| 7     | First City Monument Bank | 419 | 15     |
| 8     | Heritage Bank PLC | 378 | 13     |
| 9     | Keystone Bank Limited | 316 | 11     |
| 10    | Providus bank | 321 | 11     |
| 11    | Skye Bank   | 339    | 12     |
| 12    | Stanbic IBTC Bank Nigeria Limited | 419 | 15     |
| 13    | Standard Chartered Bank Limited | 411 | 14     |
| 14    | United Bank for Africa | 644 | 23     |
| 15    | Sterling Bank | 479 | 17     |
| 16    | Union Bank of Nigeria | 774 | 27     |
| 17    | Unity Bank PLC | 607 | 21     |
| 18    | Wema Bank   | 410    | 14     |
| 19    | Suntrust Bank Limited | 379 | 13     |
| 20    | Guaranty Trust | 442 | 16     |
| 21    | Zenith Bank | 880    | 31     |
|       | Total       | 11025  | 386    |

Table 3: Population Distribution of the Banks

Source: Field Survey, 2018

8. Instrument of Data Collection

The primary and secondary data collection methods were utilized in obtaining relevant data for the study.

Primary data are those which are collected for the first time and so are in crude form while secondary data are those which have already been collected.

The primary data collection method involved personal oral interview of users of the platform of data traffic control by the researcher. This is an indirect method of collecting primary data. Here information is not collected directly from the source but by interviewing persons closely related with the problem. This deals with asking questions to know some of the methods used in securing data in the banking system. The questionnaire method was also used to obtain the users’ view on the extent of effectiveness of the current system for data traffic control based on the performance indicators.

Secondary sources are data that already exists. The secondary data collection method involved the use of the following means to obtain relevant information for the work.

- Previous research as seen in review of related literature
- Official statistics such as fraud reports and incidences on the existing system of data traffic control in Nigerian banks for fourteen years.
- Web /internet information as seen in literature review.
- Historical data and information as seen in historical framework.

9. Z-Test

The questionnaire from the users of the existing system will be interpreted with Z-test such that each sample mean is taken and subtracted from the null hypothesis value. If there is no difference between the sample mean and null value, the value of the entire ratio equals zero.

As the difference between the sample mean and the null hypothesis mean increases in either the positive or negative direction, the strength of the value increases. This will be used to find out whether the present security measure has a significant challenge in providing security in e–payment transactions based on the performance indicators.
10. Result of Analysis of Challenges of Existing Cyber Security Platforms

This deals with the presentation and analysis of data generated in the study. The result of the analysis of data related to the research question is presented and the responses are computed statistically and presented in tables.

| S/N | Banks                | Distributed Questionnaire | Returned | Unreturned/ Uncompleted |
|-----|----------------------|---------------------------|----------|-------------------------|
| 1   | Access Bank          | 27                        | 27       |                         |
| 2   | Citibank             | 12                        | 12       |                         |
| 3   | Diamond Bank         | 24                        | 24       | 1                       |
| 4   | Ecobank              | 19                        | 19       |                         |
| 5   | Fidelity bank        | 25                        | 25       | 1                       |
| 6   | First Bank of Nigeria| 26                        | 26       | 1                       |
| 7   | First City Monument Bank | 15                  | 15       |                         |
| 8   | Heritage Bank PLC    | 13                        | 13       |                         |
| 9   | Keystone Bank Limited| 11                        | 11       |                         |
| 10  | Providus bank        | 11                        | 11       |                         |
| 11  | Skye Bank            | 12                        | 12       |                         |
| 12  | Stanbic IBTC Bank    | 15                        | 15       |                         |
| 13  | Standard Chartered Bank | 14                 | 14       |                         |
| 14  | United Bank for Africa| 23                       | 23       | 1                       |
| 15  | Sterling Bank        | 17                        | 17       |                         |
| 16  | Union Bank of Nigeria| 27                        | 27       | 1                       |
| 17  | Unity Bank PLC       | 21                        | 21       | 1                       |
| 18  | Wema Bank            | 14                        | 14       |                         |
| 19  | Suntrust Bank Limited| 13                        | 13       |                         |
| 20  | Guaranty Trust       | 16                        | 16       |                         |
| 21  | Zenith Bank          | 31                        | 31       | 2                       |
|     | Total                | 386                       | 378(98%) | 8 (2%)                  |

*Table 4: Firm by Firm Analysis of Distributed Questionnaire
Source: Field Survey, 2018*

From Table 3 above, it shows that 98 percent of the copies of questionnaire were completed and returned while 2 percent of the copies of questionnaire were not returned. This shows that high percentage of the questionnaire was returned.

11. Research Question

To what extent does the existing system perform in relation to the identified performance indicators?

| S/N | Items                                             | SA(%) | A(%) | UD(%) | D(%) | SD(%) | Total          |
|-----|---------------------------------------------------|-------|------|-------|------|-------|----------------|
| 1   | The daily and periodic monitoring results are okay.| 57(15)| 103(27) | 14(4) | 104(27) | 100(27) | 378(100%)     |
| 2   | Few of our new technologies have securities embedded in them. | 211(56) | 118(31) | 5(1) | 30(8) | 14(4) | 378(100%)     |
| 3   | We experience many false alarm scenarios.         | 143(37) | 175(47) | 12(3) | 29(8) | 19(5) | 378(100%)     |
| 4   | Our customers are not very satisfied.             | 245(66) | 86(22) | 19(5) | 11(3) | 17(4) | 378(100%)     |
| 5   | Our executive management reports on frauds are satisfying. | 65(17) | 109(28) | 30(8) | 140(37) | 34(9) | 378(100%)     |
| 6   | All attacks are always detected.                  | 49(13) | 168(44) | 5(1) | 112(30) | 44(12) | 378(100%)     |
| 7   | I will want a better system.                      | 114(30) | 149(39) | 5(1) | 28(7) | 82(22) | 378(100%)     |
| 8   | The existing system does not use much integrated platforms. | 197(52) | 132(35) | 23(6) | 8(2) | 18(5) | 378(100%)     |
| 9   | I believe that e-payment users need a better system. | 185(49) | 89(24) | 80(21) | 12(3) | 12(3) | 378(100%)     |
| 10  | The existing system is complex to use.            | 77(20) | 50(13) | 5(1) | 136(49) | 100(25) | 378(100%)     |
| 11  | We have many successful attacks.                  | 152(40) | 107(28) | 11(3) | 95(25) | 13(3) | 378(100%)     |
| 12  | We have lost much money to e-payment fraud.       | 201(53) | 99(26) | 11(3) | 50(13) | 17(5) | 378(100%)     |

*Table 5: Response on the Extent the Existing System Perform in Relation to the Identified Performance Indicators
Source: Field Survey, 2018*
12. Test of Hypotheses

Decision rule: We accept the null hypothesis when the probability value is greater than the alpha value 0.05, otherwise we reject it.

12.1. Hypotheses I

- H₀: The present security strategy has no significant challenge in providing security in e-payment transactions.
- H₁: The present security strategy has a significant challenge in providing security in e-payment transactions.

The statistical analysis is presented in table 6 below.

| Variable         | Sum of Squares | df | Mean Square | F    | Sig. |
|------------------|----------------|----|-------------|------|------|
| Between Groups   | 18.333         | 11 | 1.667       | .660 | .017 |
| Within Groups    | 271014.400     | 48 | 5646.133    |      |      |
| Total            | 271032.733     | 59 |             |      |      |

Table 6: ANOVA Table and Test of Homogeneity of Variances

| Test of Homogeneity of Variances |
|----------------------------------|
| Variable                        |
| Levene Statistic                |
| df1                             |
| df2                             |
| Sig.                            |
| .927                            |
| 11                              |
| 48                              |
| .523                            |

From the analysis above, it shows that the probability value (0.017) is less than the alpha value (0.05), the researcher therefore reject the null hypothesis and conclude that the present security strategy has a significant challenge in providing security in e-payment transactions.

13. Result Discussion on Research Question and Hypothesis

The results of the work were also discussed in relation to the research question earlier raised.

13.1. Research Question

To what extent does the existing system perform in relation to the identified performance indicators?

Table 5 gives the response on the extent the existing system performs in relation to the identified performance indicators. It shows that 15 percent of the respondents strongly agreed that the daily and periodic monitoring results are okay, 27 percent agreed that the daily and periodic monitoring results are okay, 4 percent were undecided, 27 percent disagreed that the daily and periodic monitoring results are okay while 27 percent strongly disagreed that the daily and periodic monitoring results are okay.

The analysis shows that 56 percent of the respondents strongly agreed that few of their new technologies have securities embedded in them, 31 percent agreed that few of their new technologies have securities embedded in them, 1 percent were undecided, 8 percent disagreed that few of their new technologies have securities embedded in them while 4 percent of the respondents strongly disagreed that few of their new technologies have securities embedded in them.

Also the analysis shows that 37 percent of the respondents strongly agreed that they experience many false alarm scenarios, 47 percent agreed that they experience many false alarm scenarios, 3 percent were undecided, 8 percent disagreed that they experience many false alarm scenarios while 5 percent of the respondents strongly disagreed that they experience many false alarm scenarios.

Also the analysis shows that 66 percent of the respondents strongly agreed that their customers are not very satisfied, 22 percent agreed that their customers are not very satisfied, 5 percent were undecided, 3 percent disagreed that their customers are not very satisfied while 4 percent of the respondents strongly disagreed that their customers are not very satisfied.

Also the analysis shows that 17 percent of the respondents strongly agreed that their executive management reports on frauds are satisfying, 28 percent agreed that their executive management reports on frauds are satisfying, 8 percent were undecided, 37 percent disagreed that their executive management reports on frauds are satisfying while 9 percent of the respondents strongly disagreed that their executive management reports on frauds are satisfying.

Also the analysis shows that 13 percent of the respondents strongly agreed that all attacks are always detected, 44 percent agreed that all attacks are always detected, 1 percent were undecided, 30 percent disagreed that all attacks are always detected while 12 percent of the respondent strongly disagreed that all attacks are always detected.

Also the analysis shows that 30 percent of the respondents strongly agreed that they will want a better system, 39 percent agreed that they will want a better system, 1 percent were undecided, 7 percent disagreed that they will want a better system while 22 percent of the respondents disagreed that they will want a better system.

From the analysis above, it shows that 52 percent of the respondents strongly agreed that the existing system does not use much integrated platforms, 35 percent agreed that the existing system does not use much integrated platforms, 6 percent were undecided, 2 percent of the respondents disagreed that the existing system does not use much
integrated platforms while 5 percent of the respondents strongly disagreed that the existing system does not use much integrated platforms.

The analysis shows that 49 percent of the respondents strongly agreed that e-payment users need a better system, 24 percent agreed that e-payment users need a better system, 21 percent were undecided, 3 percent disagreed that e-payment users need a better system.

The analysis shows that 20 percent of the respondents strongly agreed that the existing system is complex to use, 13 percent agreed that the existing system is complex to use, 1 percent were undecided, 49 percent disagreed that the existing system is complex to use while 25 percent of the respondent strongly disagreed that the existing system is complex to use.

The analysis shows that 40 percent of the respondents strongly agree that they have many successful attacks, 28 percent agreed that they have many successful attacks, 11 percent were undecided, 25 percent disagreed that they have many successful attacks while 3 percent of the respondents strongly disagreed that they have many successful attacks.

Also the analysis shows that 53 percent of the respondents strongly agree that they have lost much money to e-payment fraud, 26 percent agreed that they have lost much money to e-payment fraud, 3 percent were undecided, 13 percent disagreed that they have lost much money to e-payment fraud while 5 percent of the respondent strongly disagreed that they have lost much money to e-payment fraud.

Therefore, the null hypothesis was rejected and it was concluded that the present security strategy has a significant challenge in providing security in e-payment transactions. This agrees with APWG (2015) which notes that electronic fraudsters had invaded Nigerian banking environment, deploying over 185 fake mobile applications on the websites of 15 out of 17 deposit money banks with which they are extracting customers' personal and financial information with intent to steal billions of naira from bank accounts. It equally agrees with NIBSS (2015) which reveals that there was 85 percent success in fraud attempts and also notes that automated teller machines (ATMs) had most fraudulent transactions while Internet banking fraud loss was put at N3.2 billion within the last three years.

14. The Way Forward

Having considered the challenges inherent in existing cyber security platforms, there is a need to provide a solution to e-payment frauds through the use of firewalls and cryptography as a hybrid cyber security platform. Considering the various threats that seek to exploit a vulnerability to obtain compromise or destroy an information asset, an integration of competent platforms is paramount. Therefore the Human Identity-Based Firewall (HIBF) and its Media Access Control (MAC), the firewall configured with an Intrusion Detection Prevention System (IDPS) having a honey pot technology coupled with SHA-3 hashing standard will provide adequate security to the banking system. The resultant effect is a protected cyber security environment and confidence in the users of e-payment. The Central Bank of Nigeria (CBN) can benefit from this research as it will add a new vigor to her ongoing reforms to combat e-payment frauds which pose a challenge to the financial industry and are a potential threat to the overall security of the nation.

15. Conclusion

This study is of the opinion that for our banking system to be secure there is the need to employ an integrated cyber security platform for use in controlling data traffic. These technologies involve the use of Human Identity-Based Firewall which goes beyond the use of Media Access Control addresses but uses users’ profiles too to control access. They also involve the use of Intrusion Detection Prevention System which provides a proactive response to attacks. Honey pot technology should equally be implemented to be able to track and deceive intruders in the network. In order to provide a secure encryption, the Secure Hash Algorithm 3 needs to be deployed.

The honey pot security mechanism detects, deflects and counteracts attempts at unauthorized use of the banking system. It consists of data that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked. Databases often get attacked by intruders using SQL injection. Hence, honey pot architectures are such that the intruder runs against a trap database while the web application remains functional. The honey pot is placed inside the network to improve the overall state of security.

16. References
i. Anti-Phishing Working Group (2014) e-Crime Report
ii. Anti-Phishing Working Group (2014) e-Crime Report
iii. Babatunde, R.S.; Adewole, K. S.; Abdu, R.S.; Adewole, K. S.; Abdulnasim, S. O.; Isiaka, R. M.(2002) Development of an Intrusion Detection System in a Computer Network. International Journal of Computers and Technology, 2002.
iv. Byido, G.; Tzviraz, M. (2007) Analysis of Intrusion Prevention Data for Predicting Hostile Activity in Computer Networks. Communication of the ACM April 2007/Vol.50, No.4
v. Cao, B; Zhihong, Z; Tie, L; Zhongde, Y and Jiren, L. (2009) “A Study on Performance Improvement of Gateway Anti-Virus System Based on File Scanning,” Control and Decision Conference 09, pp. 2293-2295.
vi. Delloite Center for Financial Services (2015) Phishing and Insider Threats. http://www.dupress.com
vii. Delloite Center for Financial Services (2014) Mobile Financial Services: Raising the Bar on Consumer Engagement. http://www.dupress.com
viii. Deris, S, Alan Yaseen, I., Mohd. Y., Kamarulnizam, A. and Abdul, H. (2012) Intrusion Prevention System: A Survey Journal of Theoretical And Applied Information Technology 15 June 2012. Vol. 40 No.1
ix. Domke, F. (2014) Thank You Datel for Verifying the Hash.http://www.en.wikipedia.org.

x. Dutkevych, T. Piskozub, A. and Tymoshyn, N. (2007) “Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks,” IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Application, 2007, pp. 599-602.

xi. Eichlsee, M. and Mendl, F and Schlaffer, M (2014). Branching Heuristics in Differential Collision Search with Applications to SHA-512. Cryptology ePrint Archive: Report 2014/302

xii. El-Safi, A. A. (2013). Mobile Banking Project. Sudan: Faculty of Mathematical Sciences, University of Kharthoum.

xiii. Faisal, K. (2015) How do banks use encryption in ATMs and where does a bank store the data? https://www.quora.com.

xiv. Fuchsbberger, A. (2005) “Intrusion Detection Systems and Intrusion Prevention Systems,” Information Security Technical Report, vol. 10, 2005, pp. 134-139

xv. Ghorbani, T.; Lu, W. (2009), Network Intrusion Detection and Prevention: Concepts and Technique, Springer.

xvi. Guillen, E. Padilla, D. Colorado, Y. (2009) “based Intrusion Detection and Prevention Systems,” Latin-American Conference Communications, pp. 0-4.

xvii. Ido, G., Tzvi, R., Moshe, Z., (2007) “Analysis of Active Intrusion Prevention Data For Predicting Hostile Activity in Computer Networks”, Communications of the Acm April 2007/Vol. 50, No. 4

xviii. Jeremy, K. (2006). “Breach Security acquires rival firewall ModSecurity”. InfoWorld. http://www.infoworld.com

xix. Jindeon, K., Kitae, J., Jaechal, S., Seokhie, H. and Kyngho, L. (2013). Collision Attacks on AES 192/256, Eurocrypt 2012, Y2.6, m Crypton 96/128, and Anubis. Journal Applied Mathematics, Volume 2013, Article ID 71376, http://dx.doi.

xx. Lawal O. B., Ibitalo, A.and Longe, O. B. (2013). Internet Banking Authentication Methods in Nigeria Commercial Banks. African Journal of Computing and ICT, March 2013. Vol. 6.No.

xxi. Mendel, F; Nad, T and Schlaaffer, M (2013) Improving Local Collisions: New Attacks on Reduced SHA-256 Eurocrypt Conference 2013https://www.iacr.org/conferences

xxii. National Institute of Standards and Technology Computer Resource Center (2012), NIST’s policy on Hash Functions, accessed September 28, 2012.

xxiii. Nigerian Interbank Settlement Scheme-NIBSS (2015) E-Payment Fraud Landscape in Nigeria A Summary and Analysis of Reported E-Payment Frauds. Www.Nibss-plc.com.nG

xxiv. Nigerian Interbank Settlement Scheme (2014) e-payment Fraud Landscape Report. Retrieved from http://www.nibss-plc.com

xxv. Nong, Y., Syed, M. E., Qiang, C., and Sean, V. (2002), “Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection”, IEEE Transactions on Computers, VOL 51, NO. 7, JULY 2002.

xxvi. Nwogu, E. R. (2014). Improving the Security of the Internet Banking System Using Three-Level Security Implementation. IJCITS.

xxvii. Ollmann, G. (2003) “Intrusion Prevention Systems (IPS) destined to replace legacy routers,” Network Security, vol. 11, pp. 18-19.

xxviii. Popskic,V.(2016) Application Layer Firewalls. https://www.howdoesinternetwork.com.

xxix. Salah, K and Kahtani, A. (2010) “Performance evaluation comparison of Snort NIDS under Linux and Windows Server,” Journal of Network and Computer Applications, vol. 33, Jan. 2010, pp. 6-15.

xxx. Schneier, Bruce (2015) SHA-1 free start collision. Schneier on Security. https://www.schneier.com

xxxi. Schultz, E.E. and Ray, E. (2007) “Future of Intrusion Prevention,” Computer Fraud & Security, pp. 11-13.

xxxii. Suleiman, B. (2014) Payments Systems Vision 2020-Creating Enabling Environment through Regulatory Framework. http://www.vanguardngr.com

xxxiii. Stakhanova, A. Basu, S., and Wong, J. (2007) “A taxonomy of intrusion response systems,” International Journal and Computer Security, vol. 1, 2007, pp. 169-184.

xxxiv. Stevens, M. (2012). "Attacks on Hash and Applications" (PDF). PhD thesis. https://marc-stevens.nl/research/papers

xxv. Stevens, M.; Burszttein, E.; Karpman, P.; Albertini, A, and Markov, Y. (2017) “The first collision for full SHA-1” (PDF). Shattered IO. https://shattered.io/static/shattered.pdf

xxvi. Suchita, P. and Meshram (2012) IDS vs IPS IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol. 2, No. 1, 2012 86

xxvii. Suresh, N. Chari, C. and Pau-Chen C. (2003), “Bluebox: A Policy-Driven, Host-Based Intrusion Detection System”, Acm Transactions on Information and System Security, Vol. 6, No. 2, May 2003.

xxviii. Villegas, M.O. (2016) Why are cyber security KPIs Important for enterprises to determine, RSA conference, 2016

xxix. Weinsberg, Y; Tzur-David, S. Dolev, D. and Anker, T. (2016) “High Performance String Matching Algorithm for a Network Intrusion Prevention System (NIPS),” High Performance Switching and Routing, IEEE, 2006, pp. 147-153.
Appendix - Questionnaire

Dear Respondent,
Please express how much you agree or disagree with a particular statement. The research is on integrated cyber security platform for data traffic control in Nigerian banking system. Tick ✓ on the desired choice. SD=Strongly Disagreed, D=Disagreed, U=Undecided (Uncertain), A=Agreed and SA=Strongly Agreed. They have points 1,2,3,4 and 5 respectively. Please note that only the researcher will have access to your personal data. However, you may choose to be anonymous.

Thanks
Uzukwu Joy (Researcher)

SECTION A - PERSONAL DATA
Please fill in the following personal data.
Name
Bank/Company/Institution Name
Rank/Status
Level of Knowledge in Cyber Security

Beginner □ Average □ Expert □

SECTION B - QUESTIONNAIRE
Questionnaire A
The aim is to determine to what extent the existing system (the one you use for e-payment fraud controls) perform.
Select the security platform(s) you use for e-payment fraud controls.
Intrusion Detection System (IDS) □, Intrusion Prevention System (IPS) □
Layer 7 firewall □, Secure Hash Algorithm -1 □, Secure Hash Algorithm -2 □
Others (Specify) □□□□□□□□□□□□□□□□□□□

Likert scale

| S/NO | ITEMS                                                                 | SD (1) | D (2) | U (3) | A (4) | SA (5) |
|------|----------------------------------------------------------------------|--------|-------|-------|-------|--------|
| 1    | The daily and periodic monitoring results are okay.                   |        |       |       |       |        |
| 2    | All our new technologies have securities embedded in them.            |        |       |       |       |        |
| 3    | We experience many false alarm scenarios.                             |        |       |       |       |        |
| 4    | Our customers are not very satisfied.                                 |        |       |       |       |        |
| 5    | Our executive management reports on frauds are satisfying.            |        |       |       |       |        |
| 6    | All attacks are always detected.                                      |        |       |       |       |        |
| 7    | I will want a better system.                                          |        |       |       |       |        |
| 8    | The existing system does not use much integrated platforms.          |        |       |       |       |        |
| 9    | I believe that e-payment users need a better system.                  |        |       |       |       |        |
| 10   | The existing system is complex to use.                                |        |       |       |       |        |
| 11   | We have many successful attacks.                                      |        |       |       |       |        |
| 12   | We have lost much money to e-payment fraud.                           |        |       |       |       |        |