Jurnal Akuntansi, Keuangan, dan Manajemen (Jakman)
ISSN 2716-0807, Vol 4, No 1, 2022, 15-27 *https://doi.org/10.35912/jakman.v4i1.1527*

Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks

Odukwu Victory Chika[1*], Eke Promise[2], Chukwumati Mike N[3]
Department of Accounting, Faculty of Management sciences, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Rivers State, Nigeria[1,2,3]
victorychika0519@gmail.com[1], promiseeke40@gmail.com[2]

Article History
Received on 28 October 2022
1st Revision on 17 November 2022
2nd Revision on 29 November 2022
3rd Revision on 2 December 2022
Accepted on 19 December 202

Abstract

Purpose: The purpose of this research was to investigate the impact of cyber-security on fraud prevention in Nigerian commercial banks.

Method: The researcher collected primary data through the interview (WhatsApp video call) conducted with the senior employees of the respective commercial banks who know the subject matter**.**

Result: The outcomes of the research demonstrated that cloud security statistically increases fraud prevention in Nigeria**;** also, that application security statistically increases fraud prevention in Nigeria.

Contributions: it was suggested that Nigerian financial industry should be able to effectively detect fraudulent transactions and prevent them from causing financial or reputational damage to the customers or other financial institutions (FI), also, there should be a special awareness program to educate the public on how to always use strong passwords for their devices to prevent hacking, loss of money, or other resources.

Novelties: The variables adopted in this study as well as the sample size, results, and recommendations have not been used by eminent scholars in this manner.

Limitations: the results of this study would be limited to commercial banks in Nigeria, and therefore may not apply to other sectors of the economy. Similar studies were suggested to be carried out, covering other sectors of the economy to validate these results.

Keywords: *Cyber Security, Cloud Security, Application Security, Fraud Prevention, Commercial Banks*

How To Site: Victory, C. O., Promise, E., Mike, C, N (2022). Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks. *Jurnal Akuntansi, Keuangan dan Manajemen*, 4(1), 15-27.

1. Introduction

Fraud is a scourge that has severely impacted Nigeria's banking industry and the economy as a whole. Its severe effects may be seen in the declining bank income statement and the nation's economic downturn. Badejo, Okuneye, and Taiwo (2018), opined that, since deceptive activities have been increasing recently, it appears that efforts to identify and eliminate fraud in the financial sector have been largely ineffectual. Nugraha and Bayunitri (2020), describes fraud as "intentional activity by one or more individuals among management, staff, or third parties that might result in a financial statement deceit." Manipulation, fabrication, or alteration of supporting documentation; asset misappropriation; fraudulent practices including the concealment or the absence of transaction consequences from records or documents; transaction documentation that is devoid of substance; and accounting standards that are distorted (Badejo et al., 2018). Fraud prevention is the process of identifying suspicious transactions in the banking industry and preventing them from inflicting financial or reputational harm to the clients or other financial institutions (FI). As online and mobile banking grows, more prevalent and financial institutions continue to digitize, it will become even more critical to have a solid fraud protection plan. Cybercrime and fraud prevention are inextricably linked and evolving.

The entire world particularly the banking industry has benefited from the dynamic pace and result-oriented character of information technology, as well as its exponential multi-dimensional relevance, which continues to flex human activities in many fields and ages. Digital technologies and internet of things are at the center of this planned revolution. As the Internet became more widely used for commercial purposes, the quantity and variety of computer crimes grew. Although, one aspect of a crime may have been conducted via an electronic device, in certain instances, the majority of crime is perpetrated online or through technological process. According to Ahmed, Al-Khater, Al-Maadeed, Sadiq, and Khan (2020), cybercrime refers to crimes that take place in the internet's cybernetic community, commonly known as cyberspace. These rising levels of fraud and crime forced the development of cyber-security, which aims to reduce, if not eliminate, cyber-fraud and other related crimes in today's ever-changing human society.

Since most businesses, particularly those in the banking industry, are now embracing cloud computing for a variety of purposes, the security of the cloud is critical. According to Gartner, the worldwide public cloud market will grow by 23.1 percent in 2021, demonstrating that these services are frequently utilized. Between 2019 and 2021, the majority of businesses adopted their operations on a cloud-based transaction. IT professionals are hesitant to move more owing to the migration of data and applications to the cloud security, management, and compliance risks associated with cloud-based storage. They are afraid that highly confidential companies accidental leak information about persons and organizations which may result in the exposure of financial information and intellectual property.

Cloud security safeguards customer orders, blueprints, and financial information. Breach of data and theft must be avoided at all costs to preserve customer trust and secure the assets that allow you to gain a competitive advantage. The promise of cloud-based security securing data and resources is crucial for any firm moving to the cloud. Any business that wants to keep its data and applications safe from crooks should invest in cloud computing security. Businesses may gain the advantages of cloud computing, which are now widely acknowledged, by maintaining a robust cloud security stance. Cloud security comes with its own sets of advantages, such as reduced upfront costs, lower ongoing administrative and administration costs, easier scalability, stronger stability, and availability, and better-distributed denial of service protection (DDoS).

Cloud security is a sort of cyber security that focuses on ensuring the security of cloud computing systems (Badejo et al., 2018). This involves safeguarding private data and security across internet infrastructure, applications, and platforms. Cloud service providers and their customers' efforts are aimed at ensuring how a person, banks, or an organization goes about protecting these systems. To host services on their servers, cloud providers employ an all-time internet connections; since their business depends on customer trust, they utilize cloud security to keep client information private and safe. The customer, on the other hand, has some control over cloud security. Understanding these factors is required for a solid cloud security solution. Legal experts have historically argued over whether offenders are specialists, conducting one crime or related crimes on a regular basis or committing any crime in response to opportunity and external provocation. Cybercrimes, or misdeeds made possible by digital technological advances, have not yet been the subject of such fundamental research (Leukfeldt & Holt, 2022).

Another significant control measure is internal control. Internal control is an interlocking set of activities that are carried out by the board of directors, management, and other personnel (Nugraha & Bayunitri, 2020). It is designed to provide confidence in achieving certain goals within the organization. Fraud Prevention is a precautionary measure by creating policies, procedures, organization, control techniques, and employee participation. According to them, a company has internal control in an effort to supervise their business activities to create secure and successful entity-winning practices. In the field of banking, in addition to the other regulations laid down by the financial service authority as a State Institution which oversees financial institutions in Indonesia, internal controls are certainly essential. According to Jeetendra (2017), the internet has transformed the way people use traditional devices from the past. Televisions can be used for more than just watching popular television series and movies; they can also be used to call or video chat with friends through the internet. Also, mobile phone is used for more than just making phone calls; it may also be utilized to watch the latest movie. We can stay linked to everybody, regardless of where we are. Working parents can keep an eye on their kids at home and assist them with their assignments. With the push of a button, a businessman may keep a check on his employees, office, shop, and other assets (Badejo et al., 2018).

Significantly, the impact of information technology (IT) on all aspects of human and economic activities is deserving of attention and should not be overlooked. Through the use of electronics and the internet, information technology has integrated various economies across the globe (Ibrahim, 2019). In his opinion, information technology and computer networks are now used by many organizations, including banks, to perform both basic and complex activities. The electronic economy is now open to everyone, even criminals. The bulk of successful intrusions, according to various studies, target exploitable vulnerabilities in the application layer, underscoring the necessity for company IT personnel to be extremely diligent about application security. To make matters worse, the scale and diversity of apps are increasing. Defending desktop apps and static websites, which were relatively harmless and easy to target and protect ten years ago, was the application security challenge. Due to outsourced development, the number of legacy programs, and in-house development that uses 3rd party, commercial, off-the-shelf, and open-source system software, the software supply chain has become much more convoluted.

Application security is a collection of procedures, technologies, and practices targeted at protecting applications throughout their entire lifespan against threats (Pandey & Alsolami, 2020). To steal sensitive data, proprietary information, and confidential material, cybercriminals are organized, competent, and motivated to locate and exploit loopholes in enterprise systems. Application security can assist organizations in protecting all types of applications (legacy, desktop, web, mobile, and micro services) utilized by public and private stakeholders such as customers, partners, and workers. institutions want application security solutions that protect all of their programs, from internal ones to popular third-party apps on customers' phones. These solutions must cover the full development process as well as provide testing after an application has been deployed to detect any potential issues. Application security solutions must be able to test web applications for possible and exploitable vulnerabilities, analyze code, and assist in the security and defense management processes by promoting collaboration and facilitating communication among diverse stakeholders. Software automated tests that are simple to use and deploy are also required. Previous investigations demonstrated that 91% of cyber-threats start with a phishing attack. This is usually perpetrated via email (Muhattan, 2015). This kind of trick is often masqueraded as urgent permission or an enticing proposal to lure users into clunking on treacherous, malware-ridden connections. He further emphasized that unsolicited adverts are prohibited, and emails containing suspicious files are detected, ensuring that workers do not get frustrating, perhaps hazardous correspondence in their inboxes. Advanced systems feature "safe surfing" capabilities that validate the URL's endpoint to guarantee that clicking on it is safe for visitors.

According to Ahmed et al. (2020), 95% of cybercriminals disseminate spyware by gaining a person's trust and inducing them to visit a website, reveal login details, or download a harmful file by posing as a friend, cashier, or manager. Banks should help their staff recognize the telltale symptoms of online fraud, such as emails urging users to visit the website or pop-up advertising offering free goods in exchange for completing a personal survey. Finally, banks should encourage their employees to be skeptical about any link, file application, and webpage they come across online

Most cyber-security architectures include generic passwords. According to data from 2018, "123456 passwords" are still the most used. Hackers can readily guess login credentials and takeover accounts using "brute-force" attack tactics (Muhattan, 2015). The only way to eliminate this risk is for your personnel to use strong, unique passwords for each account. Complicated passwords that include capital and lowercase characters, digits, and symbols are excellent, but the longer the password, the better. Financial entities should also make creating passwords for several accounts a requirement. In this manner, if a hacker succeeds to get access to one account's login credentials, they won't be able to easily access another. The use of passwords can aid managers in preventing and identifying employee fraud by ensuring that they have access to the user computer's security and auditing functions. This can be accomplished by requesting a password before trying to gain access to operations that are not standard. Furthermore, to be more effective, the user password should be changed frequently. Although passwords are the oldest form of computer security, they continue to be the most effective and efficient method of regulating access (Leukfeldt & Holt, 2022).

New forms of as a consequence of improved technology, password protection has evolved in some industrialized countries. The password is based on the users' biological characteristics, often known as biometrics, such as thumbprints, voiceprints, retina patterns, and digital fingerprints. Fraud investigators, as well as forensic accountants, typically use the data mining technique for computer-assisted fraud detection. This method is a user-friendly, low-cost strategy for evaluating the complete database (Leukfeldt & Holt, 2022). Furthermore, this technique can aid in avoiding erroneous generalizations based on the available data. However, because data mining software cannot rapidly handle massive volumes of data and does not allow programmers to precisely focus suspicion on a specified type of fraud, this strategy is only ideal for a small business.

Today's fraudsters use sophisticated tactics and software to carry out their illicit activities successfully. While fraud prevention technology has advanced significantly and continues to do so, it is critical to keep attention. When a fraudster penetrates a company network and copies data from a database, this is referred to as a data breach. Customers' data, credit card details, and other personally identifiable information are often sought by fraudsters. Following the collection of this data, it is sold on the Dark Web. A fraudster's techniques may vary, even though the result is often the same. Additionally, attackers often adjust their techniques. The following are many of the most prevalent forms of fraud that continue to occur today. A denial of service (DoS) attack's objective is to exhaust the computing resources of a website, causing it to crash. A fraudster might command a botnet of hundreds or thousands of zombie computers to do routine tasks such as form filling. Malware is an abbreviation for "harmful software," is a broad term that refers to a variety of malicious software,

including viruses, ransomware, and spyware. Since the Creeper virus was originally identified in the 1970s, it has posed a danger to people and organizations.
Phishing is a method of extracting useful information from employees within an organization. The phishing message will employ an email, a text message, a phone call or any other kind of interaction to deceive the user into disclosing personal information or allowing malware to be installed on their device. Ransomware encrypts the data on your infected device and demands a ransom (Zheng et al., 2020). To get the encryption key that would enable you to recover access to your data, the fraudster will file a compensation claim. The con artist is holding your information hostage. Worse still, paying the ransom does not ensure the restoration of the encryption key. It's not unusual for a con artist to collect money and then disappear.

Cyber fraud is an unending challenge that threatens humanity's survival as well as infrastructures across nation-states (Aloraini, Nagappan, German, Hayashi, & Higo, 2019). Faced with threats and flaws that might result in billions of dollars in property damage, cash theft, and the failure of critical national infrastructures, countries are making substantial efforts to secure their cyberspace against cyber-attacks and cyber-crime (Ahmed et al., 2020). Cybercrime is on the rise around the world (Buchanan, 2016), causing billions of dollars in losses to individuals, businesses, organizations, and governments (Antonucci, 2017). Nigeria is a developing nation confronting many national security concerns, including classic military threats as well as non-traditional Famine, illnesses, erosion, marine piracy, drought, flood, terrorism, and the rise of cyber-crime both inside and without its borders are among the issues it faces.

Fraud exerts several costs on entities that are victims of it, according to empirical evidence. Banks may incur financial, reputational, and human capital losses, as well as be exposed to the possibility of insolvency (Rahman & Anwar, 2014). Fraud, on a larger scale, not only jeopardizes our country's economic situation by causing the loss of investment and resources but also jeopardizes the nation's peace and political stability. Nonetheless, although banks are working to minimize fraud costs, it is critical to ensure that they do not jeopardize the effectiveness of crucial fraud controls that are now in place. Nigerian commercial fraud prevention. The study's specific goals were to: investigate the influence of cloud security on fraud prevention in Nigerian listed financial institutions; determine the effect of application security on fraud prevention in publicly traded Nigerian financial institutions.

2. Literature Review

2. 1 Theoretical foundation

Routine Activity Theory (RAT): The theory was used in this study since child exploitation is one of the most widespread forms of cyber-crime in the world. This theory was re-appraised by Culatta, Clay-Warner, Boyle, and Oshri (2020). This view focuses on "crime opportunities" in the environment. Where a potential criminal opportunity arises, the action will occur at a time and place when a motivated offender and an acceptable target for victimization collide. This crime will ultimately take place in a location where there is no competent guardian to protect the appropriate target, which is described as a vulnerable person or unprotected property. As a consequence, the absence of any of these three situational elements should potentially prohibit the crime (Valan & Srinivasan, 2021). As a consequence, regular activity theory is seen as a macro-level theory that may be applied to a broad spectrum of crimes, as it seeks to explain the whole victimization process rather than offenders' particular reasons. In the absence of a qualified guardian who might perhaps prevent the criminals from committing a crime, the theory predicts that crime will occur when a motivated criminal comes into contact with a suitable victim. The theory suggests that changes in crime rates may be explained by the availability of suitable targets and competent guardians, and from what we can discern, the theory is agnostic about the influence of the supply of motivated criminals (Valan & Srinivasan, 2021).

2. 2 Empirical Review

In the view of Chika, Promise, and Werikum (2022), empirical review seeks to investigate the methods, results, conclusions, and recommendations of eminent researchers on same or similar research study. In this study, researchers highlighted some of the previous studies that are comparable with the present study. In the view of Leukfeldt and Holt (2022), who used a sample of 37 offender networks to study the problem of cybercrime. According to their study's findings, different cybercriminals exhibit different types of criminal activity. In that they sometimes engage in specific types of cybercrime, nearly half of the perpetrator sites in this sample proved to be computer crime specialists, the other half committed a variety of crimes both online and offline. The relative equity between expertise and adaptability, particularly in both online and offline activities, shows that designating fraudsters as a separate offender class may not be of great value. They raise the subject of what influences an offender's entry into cybercrime, whether they are specialized or general offenders, as a result of their study. Cybercrime actors, whether experts or general practitioners, were a part of larger online criminal networks that may have assisted in identifying and taking advantage of opportunities to commit fraud, ransomware, and other financial crimes.

In their research, Herrero et al. (2021), incorporated the data on internet addiction, lifestyle-routine activities (L-RAT), and self-control (SCT) theories into a single model that tackles the various vulnerabilities that make smartphone users possible victims of cybercrime. The approach, which we refer to as the dual associated with development of cybercrime exploitation, was empirically tested on a sample of mobile devices from throughout the country. Using Mplus causative modelling software, data from 2837 users of Spanish smartphones from a national survey were modeled. The r(Herrero et al., 2021)esults of the study confirm the predictions of L-RAT and SCT in explaining cybercrime exploitation (greater internet victimization in situations of high sensitivity, proximity, and appropriateness, relative unavailability of skilled guardian, and low self-control). Beyond the influence of L-RAT and SCT predictors, a significant impact of mobile phone addiction on hacking vulnerability was also noted. The potential victim of cybercrime exhibits two types of vulnerability: first, those outlined by criminological theories like L-RAT and SCT; second, those resulting from the deregulated, compulsive usage of the Web access device (smartphone in our work). Also, (Babayo, Bakri, Usman, Mohammed, & Muhammad, 2021), examined the implications of cybercrime and poor network security for Nigeria's digital age and national security from the perspective of alternative existing international discourse talks, using qualitative methodology, the study suggests that in order to deter crime, improve national security, and foster the digital economy, Nigeria should take steps to fortify its digital and cyber environment.

More so, Olaniyan, Ekundayo, Oluwadare, and Bamisaye (2021), investigated the use of forensic accounting in Nigeria as a tool for fraud detection and prevention. They used primary sources of information that covered the ten (10) years from 2010 to 2020, findings indicated that while foreign accounts do not completely control fraud detection, forensic accounting has a good and meaningful influence on fraud prevention. It was also discovered that forensic litigation had no appreciable beneficial effect on the recovery of money stolen through fraud. In their study, Ahmed et al. (2020), thoroughly examined methods for detecting and preventing cybercrime. They offered suggestions for

the creation of a cybercrime classifier that, in comparison to current methods, can identify cybercrimes more successfully.
Efiong, Inyang, and Joshua (2016), investigated the effectiveness of fraud prevention and detection mechanisms, using a survey approach to conduct a quantitative analysis of the data. The study found several strategies for reducing crime in Nigeria, including a strong internal control system.

Alao (2016), the influence of forensic auditing on financial fraud in Nigeria was examined (DMBs). The poll was conducted in a cross-sectional format. The study's participants were bank and audit business employees in Abeokuta, Ogun State. The study's findings demonstrated that forensic audit has a considerable impact on financial fraud control in Nigerian (DMBs), with a P-value of forensic audit reports considerably enhancing court adjudication on financial fraud in Nigeria, with a P value of less than 0.05, and that forensic audit reports greatly improve court adjudication on financial fraud in Nigeria. According to the findings, the use of forensic audits in Nigerians (DMBs) to fight financial fraud is still in its early phases. In a similar study titled "The influence of forensic investigative processes on corporate fraud deterrence in Nigerian banks," Onodi, Okafor, and Onyali (2015) looked at the function of forensic investigative techniques in discouraging corporate fraud in Nigerian banks. The study employed a survey research approach, relying on data from primary sources such as interviews and questionnaire administration, as well as secondary sources such as financial fraud and forgery complaints. The studies demonstrated a significant connection between forensic investigation approaches and corporate fraud deterrence. The statistics showed that forensic investigators' competence is although this is often necessary in the prosecution of fraud, it is not the case in the overwhelming majority of cases.

Adeniyi (2016), the influence of fraud on the demise of Nigerian banks was investigated. A cross-sectional survey, as well as an ex post facto research approach, were employed in the study. The study's results found that the occurrence of fraud has no significant influence on Nigerian banks' overall anticipated loss, with a P-value of 0.972, which is more than 0.05, and that the occurrence of fraud has no significant impact on Nigerian banks' total expected loss. According to the research, the amount of money involved in bank fraud cases in Nigeria is a reliable predictor of bank failure. To decrease fraud in Nigerian banks, the report advised that forensic auditors be hired. In Kwara state, Nigeria, Samuel, Pelumi, and Fasilat (2021), investigated the impact of internal control systems on preventing fraud among deposit money institutions. The target audience included all of the financial institutions in the state of Kwara. Purposive random sampling was used to define the sample frame for the study, which focused on all 17 quoted banks in Nigeria that are in the Kwara state. The study found a significant correlation between system of internal control and fraud protection of deposit money institutions in Nigeria.

Nugraha and Bayunitri (2020), investigated how much the influence of Internal Control against Fraud Prevention at Bank BRI of Cimahi City. The research method used in this study was explanatory method. The number of samples in this study were 46 employees of Bank BRI of Cimahi City. The analytical method used in this study was Partial Hypothesis Test (T-Test) with significance level of 5%. The program used to analyze data was Statistical Package for Social Sciences (SPSS) Ver20.00. According to this research, internal control has a significant effect on fraud prevention by 50.2%. Heliantono, Gunawan, Khomsiyah, and Arsjah (2020) analyzed the influence of the external auditor's moral development, continuing professional education (CPE) on fraud, and education on fraud detection. The research sample was taken randomly, and the total respondents were 171 external auditors working in public accounting firms in Indonesia. Results found that moral development and education had a significant effect on fraud detection, while CPE on fraud has no effect on fraud detection.

Finally, Badejo et al. (2018), assessed the numerous difficulties in identifying and preventing fraud in Nigeria's banking industry. According to the findings of the descriptive research, the main type of fraud in Nigeria is the looting of funds by bank directors and managers rather than a lack of sufficient motivation. Additionally, it is advised that government bolster already-existing anti-corruption organizations and improve their financial autonomy. To prevent future fraudsters, the managers and directors implicated in the fund plundering should be prosecuted. Before hiring, bank employees, proper screening should be done to assess their moral character and integrity.

Andi, Kusumanto, and Yusi (2022), investigated IoT monitoring to remotely monitor PV system output and efficiency to ensure the continuous supply to ventilators and monitors in the ICU Room of RSI Siti Khadijah Palembang. The approach implemented in this study is by installing IoT Monitoring as an automatic transfer switch to ensure the continuous supply for the load. The IoT monitoring shows the real-time production of PV panels, battery capacity, and inverter output. Hence, the operator can monitor the PV system output and decide whether to keep using sources from PV panels or switch to grid utilities during cloudy/rainy days. This study shows the effectiveness of implementing IoT monitoring for the On-Grid PV system installed on the rooftop of RSI Siti Khadijah Palembang.

3. Research Methodology

The purpose of this study was to conduct a descriptive research inquiry into appraising the impact of cyber security on fraud prevention of listed Nigerian commercial banks (2015-2021). This is because it works well when people's opinions are needed. The technique was developed because it focuses on people and their characteristics, which would aid the researcher in comprehending and explaining Nigerian commercial banks listed on the Nigerian Exchange Group. The researcher gathered primary data by conducting interviews (through WhatsApp video calls) with senior personnel of the respective commercial banks who are knowledgeable about the topic. The total population was 11 commercial banks listed in Nigeria. The analysis was carried out using partial regression with the support of SPSS version 20. With 33 respondents, the study's sample included the 11 commercial banks listed on the Nigerian Exchange Group (NXG). The study was guided by a functional effect created for the variables: the independent variable cyber security; indices such as cloud security (CLOUDSEC) and application security to analyze the impact of cyber security on fraud prevention of listed Nigerian commercial banks (APP SEC). These independent variable measures are used to measure fraud prevention linearly (FRAUD). The model's functional form expression is as follows:

Model: FRAUDPRE = f (CLOUDSEC, APPSEC) ………………………………...Eq (1)

The econometric model is expressed as:

FRAUDPRE = $a_0 + a_1$ CLOUDSEC$_t$ + a_2 APPSEC$_t$ + μ ....Eq (2)

Where: FRAUDPRE = Fraud prevention

CLOUDSEC = cloud security as a proxy for cyber security
APPSEC = application security as a proxy for cyber security
t = time period under investigation
ao = constant
a1 = parameter or explanatory variable coefficient u is an error term

4. Results and Discussions

This section of our study reveals the results and opens a discussion accordingly, to establish whether or not the empirical reviews are in tandem with the present study.

Table 1. Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
CLOUD SEC	11	1.00	5.00	2.4545	1.36848
APP SEC	11	1.00	5.00	3.0000	1.41421
FRAUD PREV	11	1.00	5.00	2.5455	1.50756
Valid N (listwise)	11				

Source: SPSS version 25

Cloud security had a mean value of 2.4545 and a standard deviation of 1.36848, as shown in Table 1. Fraud prevention had a mean value of 2.5455 standard deviations of 1.50756, and fraud prevention had a minimum value of 1.00 maximum value of 0.5; cloud security had a mean value of 3.0000 standard deviations of 1.41421, and application security had a minimum value of 1.00 maximum value of 0.5; fraud prevention had a mean value of 2.5455 standard deviations of 1.50756, and fraud prevention had a minimum value of 1.00 maximum value of 0.5.

Table 2. Model Summary

Model	R	R Square	Adjusted R Square	Std. The error in the Estimate
1	.77^{a}	.755	.744	.32179
a. Predictors: (Constant), APP SEC, CLDSEC				

Source: SPSS version 25

Table 2 shows the suitability of the regression model used to explain the phenomenon under investigation. The factors of cloud security and application security were determined to be adequate in explaining fraud prevention. The high value of r (0.77) indicates that the predictor factors have a significant impact on fraud prevention. The R-square of 0.755, also known as the coefficient of determination, backs this up. This suggests that cloud and application security account for 75.5 percent of the variance in the dependent variable (fraud prevention). This finding also implies that the model used to assess the influence of the factors was adequate.

Table 3. ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	17.717	2	8.859	85.552	.000^{b}
	Residual	.828	8	.104		
	Total	18.545	10			

a. Dependent Variable: FRAUDPREV
b. Predictors: (Constant), APP SEC, CLDSEC
Source: SPSS version 25

The findings of the analysis of variance are shown in Table 3. (ANOVA). The total model was statistically significant, according to the results. Furthermore, the findings suggest that the independent factors are good fraud prevention predictors. An F statistic of 85.522 and a reported p-value (0.00) that was more than the standard probability of 0.05 significant levels backed this up.

Table 4. Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.038	.219		.174	.867

CLDSEC	1.086	.164	1.092	6.634	.000
APPSEC	.117	.148	-.130	.791	.04

a. Dependent Variable: FRAUDPREV

Source: SPSS version 25

Cloud security had a calculated t-value of 6.634and a significant probability value (PV) of 0.000 > 0.05, as indicated in Table 4. As a result, the study concluded that Cloud security statistically increases fraud prevention in Nigerian commercial banks. Also, the researcher concluded that application security has a statistically significant impact on fraud prevention, 0.719 and a significant probability value (PV) of 0.04 > 0.05, respectively. As a result, the study concluded that application security statistically increases fraud prevention in Nigerian commercial banks.

Discussion:

It is crucial at this stage to discuss our findings and links them with the reviews of eminent scholars on this subject matter. Table 4 showed that cloud security had a calculated t-value of 6.634 with a criterion of the significance of 0.000 > 0.05 significant probability value (PV) The study's author gathered primary data by conducting interviews (through WhatsApp video calls) with senior personnel of the respective commercial banks who are knowledgeable about the topic. The analysis was carried out using partial regression with SPSS version 20 support. This study's results suggested that Cloud-security has a considerable and favorable influence on fraud prevention in Nigerian commercial banks. This research corroborated with Babayo et al. (2021), who looked at the ramifications of cyber-crime and insufficient cyber-security protection for Nigeria's digital economy and national security using research data collected from both primary and secondary sources and analysis, taking a qualitative approach.

Due to Nigeria's insufficient cyber-security competence, cyber-crime is flourishing undetected, harming the country's essential national infrastructure, resulting in widespread terrorism, posing a danger to national security and the environment's safety. To prevent crimes and improve national security and the digital economy, Nigeria should take efforts to strengthen its cyberspace and digital environment according to the article. Also, this result corroborated with the findings of Efiong et al. (2016), who investigated the effectiveness of fraud prevention and detection mechanisms, using a survey approach to conduct a quantitative analysis of the data. Their study found several strategies for reducing crime in Nigeria, including a strong internal control system. The study is also in conformity with Ahmed et al. (2020), who thoroughly examined methods for detecting and preventing cybercrime, and suggesting the creation of a cybercrime classifier that, in comparison to current methods, can identify cybercrimes more successfully.

Secondly, based on a determined t-value of 0.719 and a considerable probability value (PV) of 0.04 is greater than 0.05. The study's author gathered primary data by conducting interviews (through WhatsApp video calls) with senior personnel of the respective commercial banks who are knowledgeable about the topic. With 11 respondents, the study's population included the 11 commercial banks listed on the Nigerian Exchange Group (NXG). The total population was used in the investigation. The analysis was carried out using partial regression with the support of SPSS version 20. The researcher also discovered that application security had a positive significant influence on fraud prevention. This finding agreed with Onodi et al. (2015), who investigated the influence in Nigerian banks, using forensic investigative procedures to prevent corporate fraud similarly. The studies demonstrated a significant connection between forensic investigation approaches and corporate fraud deterrence.

The statistics showed that forensic investigators' competence is normally necessary in fraud prosecutions, but that this is not the case in the vast majority of instances. This study was also supported the by Herrero et al. (2021), who incorporated the data on internet addiction, lifestyle-routine activities (L-RAT), and self-control (SCT) theories into a single model that tackles the various vulnerabilities that make smartphone users possible victims of cybercrime, using Mplus causative modelling software, data from 2837 users of Spanish smartphones from a national survey were modeled. The results of their study confirmed the predictions of L-RAT and SCT in explaining cybercrime exploitation (greater internet victimization in situations of high sensitivity, proximity, and appropriateness, relative unavailability of skilled guardian, and low self-control).

5. Conclusion

The impact of cyber security on fraud prevention in Nigerian commercial banks was evaluated in this study. This inquiry reflects the significance of cyber security in the detection and prevention of fraudulent practices in Nigerian banking industry and the society as whole. Information technology via cyber security and its likes have massively assisted in ameliorating the level of fraud and associated crimes which has continued to take different shapes and colours in the Nigerian space. Consequent to this revelations, the study concluded that cloud security statistically boosts fraud prevention in Nigerian commercial banks. More so, that application security statistically increases fraud prevention in Nigerian commercial banks. As a result, the researcher made the following suggestions:

1. Nigerian financial industry should be able to effectively detect fraudulent transactions and prevent them from causing financial or reputational damage to the customers or other financial institutions (FI).
2. As online and mobile banking becomes more popular and financial institutions continue to digitize, a thorough fraud prevention strategy should be adopted to reduce, if not eliminate, fraudulent activities.
3. There should be a special awareness program to educate the public on how to always use strong passwords for their devices to prevent hacking, loss of money, or other resources.
4. Only a few scholars had taken interest to research in this area. Therefore, we advise that future scholars should take interest in this area to boost awareness and create resource material.

Conflict Of Interest Statement

Authors declared that there are no competing interests.

Statement Of Authorship

Authors have responsibility for conception and design of the study. The authors have approved the final article.

Limitations

The results of this study would be limited to commercial banks in Nigeria, and therefore may not apply to other sectors of the economy; and also, banks in other countries. Studies were suggested to be carried out, covering other sectors of the economy. Also, prospective studies on this topic should be conducted in other countries to validate these results.

Acknowledgment

We express our sincere joy to the Almighty God for his unending wisdom and grace that enabled us to undertake this task, even when it was not convenient for us. We also acknowledge the assistance of Dr. M. I. Attah for challenging us to carryout novel enquiries capable of plunging the country from its state of decadence, while contributing our quota to transforming the ever dynamic universe.

References

Adeniyi, A. (2016). Analysis of fraud in banks: Evidence from Nigeria. *International Journal of Innovative Finance and Economics Research*, *4*(2), 16-25.

Ahmed, A. A., Al-Khater, W. A., Al-Maadeed, S., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques.

Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research*, *4*(8), 1-19.

Aloraini, B., Nagappan, M., German, D. M., Hayashi, S., & Higo, Y. (2019). An empirical study of security warnings from static application security testing tools. *Journal of Systems and Software, 158*, 110427.

Andi, K., Kusumanto, R., & Yusi, S. (2022). IoT Monitoring for PV System Optimization in Hospital Environment Application. *Studies in Informatics, Technology and Systems*, *1*(1), 1-8.

Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities*: John Wiley & Sons.

Babayo, S., Bakri, M., Usman, S., Mohammed, K. T., & Muhammad, A. Y. (2021). Cybersecurity and cybercrime in Nigeria: The implications on national security and digital economy. *Journal of Intelligence and Cyber Security*, *4*(1).

Badejo, B., Okuneye, B., & Taiwo, M. (2018). Fraud detection in the banking system in Nigeria: Challenges and prospects. *Shirkah: Journal of Economics and Business, 2*(3).

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*: Oxford University Press.

Chika, O. V., Promise, E., & Werikum, E. V. (2022). Influence of Liquidity and Profitability on Profits Growth of Nigerian Pharmaceutical Firms. *Goodwood Akuntansi dan Auditing Reviu, 1*(1), 1-13.

Culatta, E., Clay-Warner, J., Boyle, K. M., & Oshri, A. (2020). Sexual revictimization: A routine activity theory explanation. *Journal of interpersonal violence*, *35*(15-16), 2800-2824.

Efiong, E. J., Inyang, I. O., & Joshua, U. (2016). Effectiveness of the mechanisms of fraud prevention and detection in Nigeria. *Advances in Social Sciences Research Journal*, *3*(3).

Heliantono, H., Gunawan, I. D., Khomsiyah, K., & Arsjah, R. J. (2020). Moral development as the influencer of fraud detection. *International journal of Financial, Accounting, and Management*, *2*(1), 1-11.

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International journal of environmental research and public health, 18*(7), 3763.

Ibrahim, U. (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. *NDIC Quarterly*, *34*(12), 1-20.

Jeetendra, P. (2017). Introduction to cyber security. *Uttarakhand Open University*, 978-993-84813-84896-84813.

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*, 106979. doi:10.1016/j.chb.2021.106979

Muhattan. (2015). 3 Essential types of cyber security solutions. *Manhattan tech support publishers*--www.ilovepdf.com.

Nugraha, R., & Bayunitri, B. I. (2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). *International journal of Financial, Accounting, and Management, 2*(3), 199-211.

Olaniyan, N. O., Ekundayo, A. T., Oluwadare, O. E., & Bamisaye, T. O. (2021). Forensic accounting as an instrument for fraud detection and prevention in the public sector: moderating on ministries, departments and agencies in Nigeria. *Acta Scientiarum Polonorum. Oeconomia, 20*(1), 49-59.

Onodi, B. E., Okafor, T. G., & Onyali, C. I. (2015). The impact of forensic investigative methods on corporate fraud deterrence in banks in Nigeria. *European Journal of Accounting, Auditing and Finance, 3*(4), 69-85.

Pandey, A. K., & Alsolami, F. (2020). Malware Analysis in Web Application Security: An Investigation and Suggestion. *International Journal of Advanced Computer Science and Applications*, *11*(7), 191–201. doi:https://doi.org/10.14569/IJACSA.2020.0110725

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia-Social and Behavioral Sciences*, *145*, 97-102.

Samuel, O., Pelumi, I., & Fasilat, O. (2021). Effect of internal control system on fraud prevention among deposit money banks in Kwara State, Nigeria. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(1), 264–271.

Valan, M. L., & Srinivasan, M. (2021). The application of routine activity theory in explaining victimization of child marriage. *International review of victimology*, *27*(2), 211-226.

Zheng, Y., Pal, A., Abuadbba, S., Pokhrel, S. R., Nepal, S., & Janicke, H. (2020). *Towards IoT Security Automation and Orchestration.* Paper presented at the 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA).