Innovations

Artificial intelligence as determinants of cyber security in financial institutions in an emerging economy: experienced from Deposit Money Banks in Southeast Nigeria

[1]Dr Ezuwore-Obodoekwe, Charity Nkeiru
[2]Dr Nsoke, Uche Peter
[3]Dr Anisiuba, Chika Anastesia
[4]Dr Ifeoma, Maria Ihegboro

[1,3]Department of Accountancy, Faculty of Business Administration University of Nigeria, Nsukka
[2]Department of Accountancy, Faculty of Management Sciences, University of American; in Affiliation with Peaceland College of Education, Enugu, Nigeria
[4]Department of Banking and Finance, Faculty of Business Administration University of Nigeria, Nsukka
Corresponding Author: **[4]Dr Ifeoma, Maria Ihegboro**
Received: 21 June 2022 Accepted: 27 July 2022 Published: 30 July 2022

Abstract

The recent advancement in PC architecture has changed the essence of science and engineering. This advancement is principal to such an extent that it significantly reshapes relationships among individuals and organisations and provides a foundation for understanding and learning intelligent conduct in a living and engineered framework. Artificial intelligence (AI) is the branch of software engineering that manages intelligent specialists' investigation and plan that sees its environment and makes moves that boost its accomplishment. This study examines artificial intelligence as a determinant of cyber security systems in deposit money banks in Southeast Nigeria. The study adopted the survey design method and used primary and secondary data sources. The population of the management staff of the selected banks was 2553. Sample size estimation was drawn using the Trek (2012) formula, which gives a sample size of 753. The data collected were analysed and tested using the non-parametric approach, the ordinal regression, and the Spearman rank correlation. The study's outcome revealed that artificial intelligence significantly affects the cyber security system of deposit money banks. It was concluded that artificial intelligence has positively impacted the cyber security system of deposit money banks in Southeast Nigeria. The study recommends that deposit money banks should utilise artificial intelligence effectively to enhance and solidify their cyber security system, as doing so will generate trust and confidence in the minds of their customers.

Keywords: *1. Artificial intelligence, 2. Cyber security, 3. Cyber security system; 4. Cyber security threats, 5. Emerging economy*

1. Introduction

Artificial intelligence (AI) is a notion that has been developed to replicate the human brain since it can look at many issues from a human perspective. AI is the branch of software engineering that manages intelligent specialists' investigation and plans that sees its environment and makes moves that boost its chances of accomplishment (Bostrom, 2005). As internet computing and distribution get more sophisticated, fundamental problems concerning information security and privacy are posed. Due to this issue, physical devices like detectors and sensors cannot safeguard or monitor these infrastructures. In this situation, a high-performing, flexible, reliable, and adaptable cyber defence system like AI is required. AI has been used in the banking industry for some time. AI methods are being quickly applied in the banking sector for a wide range of applications (Vishal, 2019).

The recent advancement in PC architecture has changed the essence of science and engineering. This advancement is principal to such an extent that it significantly reshapes relationships among individuals and organisations and provides a foundation for understanding and learning intelligent conduct in a living and engineered framework. This improvement is regarded as artificial intelligence (Sindhu and Namratha, 2019).

Due to the widespread use of digital technologies, considerable advancements in algorithmic skills, access to richer data, and rising processing power, the deployment of AI has significantly accelerated in recent years. AI was set up as a discipline. However, its applications have sped up in recent years, upheld by evolution in machine learning and upgrades in computing power, data stockpiling, and communication networks (David and Houghbono, 2019). An AI explosion involves executing tasks like social and business transactions, speaking, and sound recognition. Far essential techniques are assisted with performing the task, like profound learning, natural language processing, and predictive and prescriptive analysis (Soni, 2019). These strategies are used to tackle cyber security problems by observing artificial intelligence procedures (Cidon, Gavish and Perone, 2019).

According to a Gartner global survey, on September 24, 2020, a survey of about 200 business and IT professionals revealed that 24% of respondents' organisations increased their artificial intelligence investments, and 42% remained unchanged since the start of COVID-19. 14% of large companies used AI in 2019, up from 3% in 2018. As the organisation enters the renewal phase of its post-pandemic reset, 75% of respondents said they would either maintain existing AI efforts or launch new ones. Frances Karamouzis, a distinguished research vice president at Gartner enterprise, claims that investment in AI has been unabated despite the crisis. However, organisations' failure to link such investments back to economic value is the biggest obstacle to putting AI programs into production (Stamford, 2020).

Chatbots, process optimisation, and fraud analysis on transactional data are some of the most widely used AI applications. Examples of emerging applications include consumer and market segmentation, computer-assisted diagnosis, virtual agents for call centres, sentiment analysis and opinion mining, face detection and recognition, and human resources applications like resume screening. The industries that use these apps the most frequently are insurance, banks, software and IT services, telecom, and retail. Since 2015, AI startups have raised more funding rounds and typically command larger values than comparable non-AI enterprises (David and Houghbono, 2019).

Due to the increased threat of cyber-attacks, academics and professionals have been interested in the topic of cyber security. Cyber security is the organisation and collection of tools, procedures, and structures used to safeguard electronic systems from events that conflict with fundamental and legal property rights in cyberspace (Craigen, Diakun-Thibault & Purse, 2014). We are more vulnerable to cyberattacks than ever due

to the rising usage of digital gadgets and the internet in our personal and professional lives. It is challenging to distinguish cyberspace from these sectors and to pinpoint the risks because cyberspace is firmly ingrained into all other industrial sectors, facilitating interconnection. Cyberspace's growing complexity has opened up new opportunities in the economy, society, and politics (Clemente, 2013).
Siddiqui, Yadav, and Husain (2018) saw that common issues, for example, misrepresentation and theft, are attained in new forms of cyber wrongdoing through information technology. The number and assortment of cybercrimes are increasing daily. Forswearing of-service assaults, infrastructure assaults, and other issues around data protection are significant pieces of high profiling cyber assaults (Vieira and Sehgal, 2018).

About 70% of CEOs of financial institutions, particularly the capital market and banks, consider cyber security a threat to their turn of events. Security incidents affected financial service organisations more frequently than businesses in different industries. Worldwide banking and financial industry guarantee that cyber-assault consists of about $360 billion in costs in a year. In recent years, worldwide ransomware assaults have affected financial institutions.

Therefore, in a situation like this, it becomes essential to foster a couple of security projects to ensure cyber threats in financial institutions, particularly the banking sector. Most banks are truly embarking on and implementing artificial intelligence to address this. The significant goal of this paper was to examine and set up artificial intelligence as the determinant of cyber security for financial institutions in an emerging economy, focusing on selected deposit money banks in the Southeast part of Nigeria, West Africa. The specific objectives were to: determine the impact of artificial intelligence on the cyber security arrangement of deposit money banks and to ascertain the degree to which artificial intelligence has alleviated cyber security threats/attacks on deposit money banks in southeast Nigeria.

2. Review of Related Literature

2.1 Artificial Intelligence

A lot has been expounded on artificial intelligence (AI), with researchers approaching it from various points of view. Artificial intelligence is a regular strategy that can perform different functions associated with human minds like reasoning, learning, interaction with the environment, exercising, creativity, perceiving and problem-solving (Soni, 2019). According to Kaya, Schildbach, AG and Schneider (2019), artificial intelligence has been created to emulate the human brain. AI can investigate many problems with a comprehensive human methodology.

An artificial intelligence term was coined by John McCarthy in 1956. He defines it as "the science and engineering of making intelligent machines". He further expresses that artificial intelligence is the branch of software engineering that manages the examination and plan of intelligent specialists that see their environment and makes moves that amplify their chances of accomplishment. He further gave a rundown of AI as the capacity to simultaneously hold two different ideas in mind and still retain the ability to function (McCarthy,1956).

2.2 AI and the Banking System

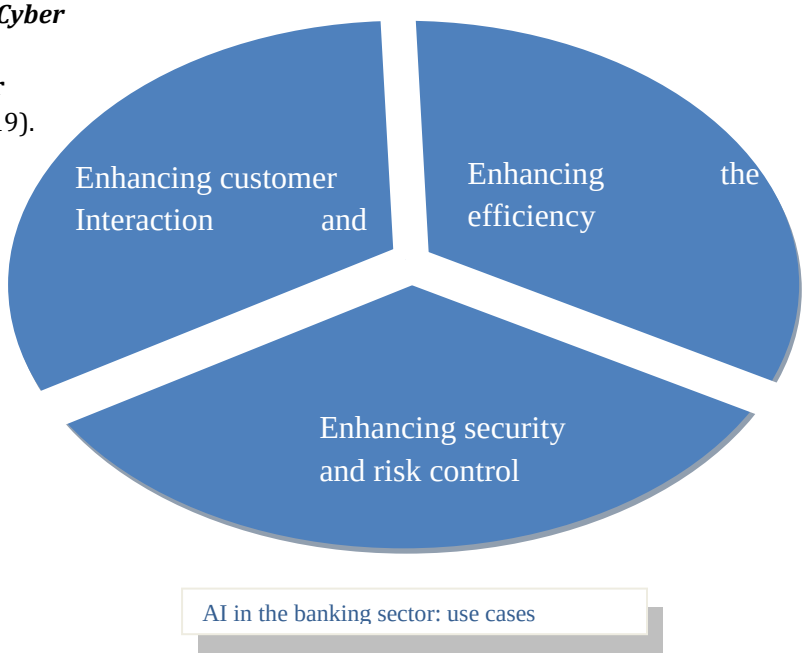
Banks are being compelled to change their business models due to the entry of new FinTech players. Through this reformation, they have been able to offer more competitive products and better service by integrating financial technologies (Caron, 2019). The industry has recently adopted AI due to efforts to automate procedures. The technology can be used in various fields, such as detecting fraud or money laundering (National Science and Technology Council 2016). While 50% of firms will utilise AI, according to Boobier (2020), the banking industry is thought to be among those most impacted by this technology. This is partly because the industry requires reliable analytical tools to deliver customer data, boost operational efficiency, and enhance risk management. AI has a huge potential to improve these processes and acquire competitive advantages. Singh (2020) identifies seven areas of banking where AI has the potential to change the way things are done. These facets include trading and securities, regulatory compliance, fraud and risk management, voice assistants and chatbots, customer service, customer engagement, and voice assistants and chatbots.

2.3 Use of Artificial Intelligence

Artificial intelligence procedures maintain a vast number of reality and flavours. Use cases of artificial intelligence are classified into three classifications; these classifications can give information about possible areas of chance for the banking sector. These three classifications are classified underneath:

i. Enhancing customer interaction and experience: examples are customer service improvement, voice banking, Robo-exhortation, biometric authentication, customer segmentation, and chatbots.
ii. Improving the efficiency of banking processes: examples are predictive maintenance in IT, complaints management, automated data extraction, credit scoring, measure automation, and archive classification.
iii. Developing security and risk control: examples are AML (Anti-Money Laundering) detection and monitoring, enhanced risk control, the backing of data quality assurances, cyber risk prevention, compliance monitoring, instalment transaction monitoring and extortion prevention. This is shown in the pie chart in figure 1

Figure 1: Use of AI in the Banking Sector
Source: Hasham, Joshi, and Mikkelsen (2019).



2.4 Cyber Security

Cyber security is an interaction that protects computers, workers, networks, and digital data from unapproved access and destruction or assault in cyberspace. Cyber security history traces back to the seventies before the vast majority even had a PC**.** Businesses and governments' objectives in using the cyber security component are to secure their confidential information, ensure the accessibility of the information, and maintain its integrity (Adel & Sara 2019).

Nevertheless, cyber security is critical in many organisations because of the increased reliance on technology. Accordingly, firms worldwide should know about the significance and application of cyber security. One of the main objectives of cyber security is to shield the data and information from illicit theft and harm, as these demonstrations have generally increased in recent years. A portion of the advantages of cyber security is working with crafted by the organisation, increasing customer satisfaction, reducing administrative work, and improving cash stream, well-being, and security.

According to ISACA (2017), the phrases cyber security and information security are frequently used interchangeably; however, cyber security is a piece of information security. Specifically, cyber security practice is an elective expression for IT security and information risk management. Nevertheless, cyber security is a component of information technology security. It protects computers, programs, digital data and assets from unapproved access or destruction. Ordinarily, cyber security connotes what may be anticipated to preserve and shield institutions and individuals from planned assaults, breaches, incidents and consequences.

2.5 Cyber Security and Financial Institutions

With the fast growth in the technological environment, many organisations, irrespective of their sizes, rely entirely on the use of information systems in their everyday operations. This requires the organisation to contemplate successful techniques regarding information security in a request to ensure the institution's touchy and significant databases are not taken or assaulted by cybercriminals (Adel & Sara 2019**).**

Cyber assaults are increasing and represent a substantial risk to the steadiness of the overall financial sector. Assaults increase in number, extension, and sophistication, making it hard to predict the all-out sway. The Herjavec group indicated that the worldwide annual expense of cybercrime would increase to around USD 6 trillion by 2021, from USD 400 billion in mid-2015 (Al-Alawai, Al-Bassam, and Mehrotra, 2020). In a July 2017 report, Lloyd's of London gauges that a single worldwide cyber-assault could harm the economy by USD 121 billion (Bostrom Nick, 2005). Beyond financial misfortune, cyber-assaults can disturb business and financial sectors and contribute to a more extensive loss of confidence.

Cyber assaults can affect all sections of life. As confirmed during the Wanna Crypt ransomware assaults in May 2017, more than 200,000 computers in about 150 nations, including those found within emergency clinics, utilities, railroads, telecommunications and auto companies, were influenced. Also, the June 2017 Petya ransomware affected computers within 64 nations (Hashma, Joshi and Mikkelsen, 2019). According to International business machines (IBM), the financial sector in 2016 was more assaulted than any other sector. This breached over 200 million records (Cidon, Gavish, Perone, and Barracuda, 2019).

The worldwide banking framework has confronted significant changes within the last couple of years in processes, transactions, and operations, influenced by technology and its innovations within recent trends. Notwithstanding, there are explicit concerns within foundational operations and information technology innovation. Banks depend on outsider systems to offer a few digital services. This has raised the awareness of

programmers and criminals of technological threats and shortcomings that would permit them to hack banking systems and take necessary information and assets. Cyber threats and assaults are challenging because of the fast technological change (Adel & Sara 2019).

2.6 Empirical Review

In an investigation to determine the part of artificial intelligence in combating cyber threats in the banking industry, Soni (2019) attempted to determine how implementing AI in the banking sector can mitigate cyber assaults. The investigation was an overview of 20 selected banks in Kentucky, using 200 respondents from the designated banks. The study reveals that artificial intelligence methods inform customers' conduct and interest. The legitimate plan is offered by artificial intelligence towards the banking sector, by which they are ready to recognise extortion in transactions. Artificial intelligence is directly linked with cyber security as different cybercrimes are prevented and distinguished by AI-based misrepresentation detection systems. The examination concludes that artificial intelligence conveys huge expenses and risks and removes control from humans while dehumanising actions in a few different ways.

Boer and Vazquez (2017) examined how cyber assaults could substantially affect the worldwide financial framework in another examination that glances at cyber security and financial security. The study utilised secondary information significantly from the extant literature. After a broad review of extant literature, the investigation shows that many financial framework components like banks, non-bank financial institutions, other financial services, markets, and financial market infrastructure cannot be replaced easily whenever lost or interrupted. This could prompt sudden spikes in demand for the present moment, liquidity of funding, freezes and defaults, and loss of data integrity which could disturb market movement significantly.

Xie (2019) investigated the improvement of artificial intelligence and its impact on the financial framework in Guangzhou, China, using a graphic overview. Duplicates of the questionnaire were administered to 150 respondents from 5 selected banks in Guangzhou. The investigation reveals that the fast advancement of AI and machine learning and its application has been generally used in many financial areas. This has significantly impacted the financial market, institutions and regulation. AI has carried enormous change to the entire financial industry, which creates a progression of innovative financial services like an intelligent consultant, intelligent lending, monitoring and warning, and intelligent customer service as times required. The investigation concludes that artificial intelligence is a lucky result of improving science and technology. Yet, there are corresponding challenges in applying artificial intelligence.

In yet another study, Yazbeck, Frickenstein, and Medine (2019) tried to recognise the challenges and solutions for financial inclusion. The investigation was interview-based with financial suppliers from across Africa. The study identifies four sorts of cyber assaults that frequently influence the financial institution: social engineering assault, insiders intent on causing hurt, Malware, Ransomware and Denial of service assault, and tricks. The study reveals the following as challenges that financial institutions face in managing cybercrimes: the industry is poorly prepared; approach creators' capacity constraints inhibit understanding and successful regulatory and supervision of cyber security. The examination reveals the expected solutions to cyber security in the financial sector, including government investment in building public cyber security support structures for the financial sector. Financial sector suppliers and associations are leading cooperative efforts to enhance cyber resilience. Promising cyber security initiatives are building on open private partnerships; multi-country approaches can help defeat the resource hole; however, economies of scale and degree; improvement accomplices can uphold the sector to become more cyber resilient. The examination concludes that banking services are moving to digital at a consistently faster rate; nonetheless, the sector entertainers face a growing risk from cybercriminals seeking to assault their systems and consumers.

3. Methodology

A cross-sectional survey method was adopted to seek the opinions of the management staff of the selected deposit money banks in Southeast Nigeria on artificial intelligence as determinants of cyber security in the banking industry. The Southeast region of Nigeria comprises five states: Abia, Anambra, Ebonyi, Enugu, and Imo states. The study population comprises all the deposit money banks' staff in Southeast Nigeria. A multi-stage method was used to draw the required population, which involves choosing the well-known and highly performing deposit-money banks from the population frame. Out of a population frame of twenty (20) registered deposit-money banks in Nigeria under CBN as of 2016, a total of twelve (12) deposit-money banks were selected. The total population of the management staff of the banks chosen is 2553. Using the Trek (2012) formula, a sample of 753 was selected. A well-structured questionnaire was used for the data collection. The data collected were analysed and tested using the non-parametric approach, the ordinal regression, and the Spearman rank correlation.

3.1 Models Specification

The functional model of the study is given as follows:
Cyber security (CS) is a function of artificial intelligence (AI)
Therefore:

$CS = \beta 0 + a1\ AI + \mu$ - - - - [1]

Specifically,

$CST = \beta 0 + a1\ AI + \mu$ - - - - [2]

$CSS = \beta 0 + a1\ AI + \mu$ - - - [3]

Where CS = cyber security
AI = artificial intelligence
CST = cyber security threats
CSS = cyber security system
μ = error term of the random variable
α = a constant amount
β = coefficient of the independent variable.

4. Results and Discussion

A total of seven hundred and fifty-three copies of the questionnaire were administered to the management staff of the twelve selected deposit money banks. Six hundred and ninety-nine copies of the questionnaire were retrieved, which amounted to a 92.8% response rate. Six hundred and ninety-nine copies of the questionnaire retrieved were found useable. Fifty-four copies of the questionnaire were not retrievable, which amounted to 7.2%.

4.1 Test of hypothesis

The data collected during the survey are presented, analysed and interpreted, followed by discussions of the findings.

4.2 Pre-test

Before the analysis, there is a need for a pre-test. The essence is to check if the data set is normally distributed and to know the right analytical tool for our analysis. If the data set is normally distributed, we adopt a parametric method: linear regression and Pearson correlation. On the contrary, if the data set is not normally distributed, we rely on the non-parametric approach: the ordinal regression and Spearman rank correlation. The outcomes of the pre-test are shown in the next section.

Table 1: Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
AI	699	79.3%	183	20.7%	882	100.0%
CST	699	79.3%	183	20.7%	882	100.0%
CSS	699	79.3%	183	20.7%	882	100.0%

Table 1 shows the valid, missing and total cases in the analysis. The table shows that 699 cases representing 79.3%, are valid, while 183 cases representing 16.5%, are missing out of the total cases of 882. This is good enough as 79.3% of cases are a good representation of the data and can be used for meaningful analysis

Table 2: Descriptives				
			Statistic	Std. Error
AI	Mean		1.6767	.02304
	95% Confidence Interval for Mean	Lower Bound	1.6314	
		Upper Bound	1.7219	
	5% Trimmed Mean		1.6191	
	Median		1.6000	
	Variance		.371	
	Std. Deviation		.60916	
	Minimum		1.00	
	Maximum		3.80	
	Range		2.80	
	Interquartile Range		.60	
	Skewness		1.484	.092
	Kurtosis		2.230	.185
CST	Mean		1.5906	.01483
	95% Confidence Interval for Mean	Lower Bound	1.5614	
		Upper Bound	1.6197	
	5% Trimmed Mean		1.5628	
	Median		1.6000	
	Variance		.154	
	Std. Deviation		.39200	
	Minimum		1.00	
	Maximum		3.20	
	Range		2.20	
	Interquartile Range		.40	
	Skewness		1.303	.092
	Kurtosis		3.062	.185
CSS	Mean		1.6613	.02411
	95% Confidence Interval for Mean	Lower Bound	1.6140	
		Upper Bound	1.7086	
	5% Trimmed Mean		1.5998	

	Median	1.5000	
	Variance	.406	
	Std. Deviation	.63745	
	Minimum	1.00	
	Maximum	3.75	
	Range	2.75	
	Interquartile Range	.75	
	Skewness	1.294	.092
	Kurtosis	1.638	.185

Table 2 shows the result of the descriptive statistics. Here, our interest is in skewness and kurtosis. We do this by dividing the statistics by the standard error. If the result falls between -1.96 and +1.96, then our data set is normally distributed. The result obtained after computation shows that our data set is not normally distributed. To be double sure of this result, we perform the normality test. The result is shown below.

Table 3: Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
AI	.204	699	.000	.848	699	.000
CST	.155	699	.000	.892	699	.000
CSS	.186	699	.000	.861	699	.000

The test of normality is shown in table 3. In this test, we have two test statistics, Kolmogorov-Smirnov and Shapiro-Wilk. The Kolmogorov-Smirnov is used when the data set is above a hundred. In contrast, the Shapiro-Wilk is used when the data set is below a hundred. In this study, our data set is above a hundred, so we rely on Kolmogorov-Smirnov.

Of interest is that each of the variables should not be statistically significant. From the table, our variables are less than 0.05, meaning they are statistically significant. This shows the data set are not normally distributed.

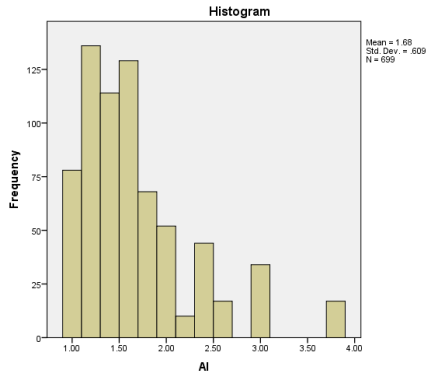


Figure One: Histogram for AI

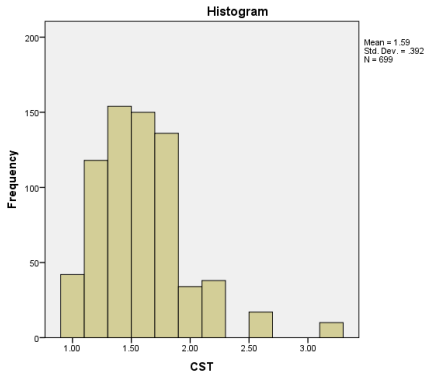


Figure Two: Histogram for CST

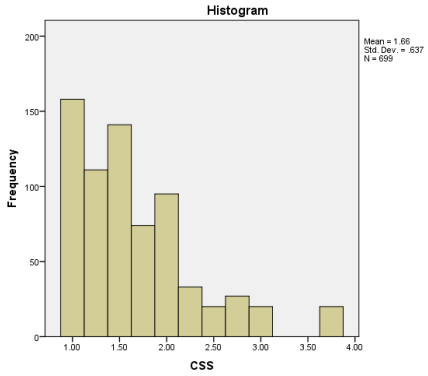


Figure One: Histogram for all variables

The histograms above further support the test result in tables 1, 2 and 3. Figures 1, 2, and 3 are the histogram for each variable. The rule is that the histogram should be bell-shaped for the variables to be normally distributed. From the histograms above, it can be concluded that all variables are not normally distributed as the histograms do not have a bell shape. Considering the facts above, we adopt ordinary regression as the appropriate tool to analyse our hypotheses.

4.3 Hypothesis 1

O1: Artificial intelligence has no significant effect on the Southeast's cyber security system of deposit money banks.

A1: Artificial intelligence significantly affects the cyber security system of deposit money banks Southeast.

Table 4: Correlations

			AI	CST	CSS
Spearman's rho	AI	Correlation Coefficient	1.000	.477**	.404**
		Sig. (2-tailed)	.	.000	.000
		N	699	699	699
	CST	Correlation Coefficient	.477**	1.000	.278**
		Sig. (2-tailed)	.000	.	.000
		N	699	699	699
	CSS	Correlation Coefficient	.404**	.278**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	699	699	699

Table 4 contains the result of the Spearman rank correlation. The test takes care of the disturbances that caused the abnormality and shows the variables' behaviour. The result shows a low and moderate correlation between the variables. The correlation among AI, CST and CSS is low and moderate. It has a value of .477 and .278 and is statistically significant. This shows a weak correlation among the variables.

Table 5: Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1249.072			
Final	1004.672	244.400	1	.000

Table 5 shows the outcome of the model Fitting information. This table tells us how well the model fits the data. The information in table 5 is statistically significant because its p.value is less than 0.05, implying our model fits the data very well.

Table 6: Goodness of Fit

	Chi-Square	df	Sig.
Pearson	377.676	79	.760
Deviance	310.762	79	.620

Table 6 shows the Pearson and deviance chi-square tests which are helpful to determine if a model exhibit good fits to the data. The non-significant nation of the p-value is an indicator that the model fits the data well. The Pearson and deviance are non-significant (.760 and .620). These values are clearly above 0.05, which clearly shows that the model fits the data set well.

Table 7: Pseudo R-Square

Cox and Snell	.295
Nagelkerke	.302
McFadden	.092

Link function: Logit.

Table 7 contains the outcome of the Pseudo R-square. Our interest here is the Nagelkerke. This is more of the R-square for linear regression. The value of .302 indicates a 30% change in CST. It implies AI adopted by the Southeast money deposit banks is responsible for a 30% change in CST.

Table 8: Test of Parallel Lines[a]

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	368.093			
General	295.738[b]	74.672	7	.324

Table 8 is the outcome of the test of parallel lines. It tests for the assumption of proportional odds. The null hypothesis is that the odds for each explanatory variable are consistent or the same across different thresholds of the outcome variable. The outcome must not be statistically significant not to violate the test of proportional odds. Our result has not violated the assumption from the outcome as the probability is greater than the 0.05 significant level. With this outcome, we can discuss the main result; parameter estimates

Table 9: Parameter Estimates

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[CST = 1.00]	.160	.245	.428	1	.513	-.320	.640
	[CST = 1.20]	1.820	.216	70.826	1	.000	1.396	2.244
	[CST = 1.40]	2.963	.224	174.520	1	.000	2.524	3.403
	[CST = 1.60]	4.080	.246	275.456	1	.000	3.598	4.561
	[CST = 1.80]	5.583	.295	357.615	1	.000	5.005	6.162
	[CST = 2.00]	6.170	.319	373.003	1	.000	5.544	6.796

	[CST = 2.20]	7.492	.392	365.692	1	.000	6.724	8.259
	[CST = 2.60]	8.783	.503	305.320	1	.000	7.798	9.768
Location	AI	1.956	.132	220.224	1	.000	1.698	2.215

Table 9 is the outcome of the parameter estimate. The independent variable, artificial intelligence (AI), is positive. It significantly affects the cyber security system of deposit money banks in the South East (1.956, .000). The regression coefficient, known as the estimate, is positive. By implication, a unit increase in AI will lead to a predicted increase of 1.956 in the Southeast's cyber security system of deposit money banks. The result revealed that AI is a significant positive predictor of the Southeast's cyber security system of deposit money banks.

4.4 Hypothesis 2

O2: Artificial intelligence has not significantly mitigated the cyber security threats of deposit money banks in the Southeast.

A2: Artificial intelligence has significantly mitigated cyber security threats of deposit money banks in the Southeast.

Table 10: Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1186.300			
Final	1082.726	103.574	1	.000

Table 10 shows that our model fits the data very well as the p-value is less than the 5% significance level.

Table 11: Goodness-of-Fit (Hypothesis)

	Chi-Square	df	Sig.
Pearson	133.482	89	.724
Deviance	972.210	89	.354

Table 11 shows the Pearson and deviance Chi-square tests. The non-significant nation of the p-value is an indicator that the model fits the data well. From the outcome, the Pearson and deviance Chi-square are non-significant (.724 and .354). These values are clearly above 0.05, which clearly shows that the model fits the data set well.

Table 12: Pseudo R-Square (Hypothesis Two)

Cox and Snell	.138
Nagelkerke	.140
McFadden	.036

Link function: Logit.

The outcome of the Pseudo R-square is shown in table 12. The value of .140 indicates a 14% change in CSS. It implies AI adopted by the Southeast money deposit banks is responsible for a 14% change in CSS.

Table 13: Parameter Estimates								
		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[CSS = 1.00]	.789	.204	15.022	1	.000	.390	1.189
	[CSS = 1.25]	1.589	.204	60.466	1	.000	1.189	1.990
	[CSS = 1.50]	2.434	.214	129.897	1	.000	2.016	2.853
	[CSS = 1.75]	2.935	.222	174.323	1	.000	2.499	3.371
	[CSS = 2.00]	3.839	.244	247.174	1	.000	3.360	4.318
	[CSS = 2.25]	4.318	.259	278.560	1	.000	3.811	4.825
	[CSS = 2.50]	4.660	.271	296.545	1	.000	4.130	5.191
	[CSS = 2.75]	5.262	.296	316.485	1	.000	4.683	5.842
	[CSS = 3.00]	6.025	.340	314.259	1	.000	5.359	6.691
Location	AI	1.301	.118	121.237	1	.000	1.070	1.533

Table 13 is the outcome of the parameter estimate. The independent variable, AI, is positive. It significantly affects the cyber security threats of deposit money banks in the Southeast (1.301, .000). The regression coefficient is positive. By implication, a unit increase in AI will lead to a predicted increase of 1.301 in the Southeast's cyber security threats of deposit money banks. The result again revealed that AI is a significant positive predictor of the cyber security threats of deposit money banks in the Southeast.

4.5 Result Implication

The study results show that artificial intelligence positively affects the cyber security system of deposit money banks. The result implies that financial institutions and deposit money banks should embrace and implement artificial intelligence in their operations as security measures. Doing this will enhance the effectiveness and solidity of their cyber security, thereby acting as agents of defence against cyber security threats and attacks.

The first hypothesis showed that artificial intelligence significantly affects the cyber security system of deposit money banks. This result implies that the effective implementation of artificial intelligence in support of the cyber security system of the deposit money banks provides information on the behaviour and interest of customers and helps to prevent cyber threats and attacks. This finding substantiates the outcome of Soni (2019), which stated that artificial intelligence techniques provide information about customers' behaviour and interest; and that proper design is provided by artificial intelligence in the banking sector, by which they can identify fraud in transactions.

The second hypothesis showed that artificial intelligence has significantly mitigated deposit money banks' cyber security threats/attacks. This result implies that with adequate and constant use and application of artificial intelligence for the enhancement and solidification of the cyber security system of deposit money banks, the trust and confidence level of customers will grow, increasing the chances of attracting more customers, retaining the existing customers and improving their patronage and loyalty. This result supported the outcome of Boer and Vazques (2017), who reported that "loss of confidence is recorded when the financial system built on the confidence and trust placed by participants is eroded. This could lead to the liquidity of funding, freezes and defaults.

5 Conclusion

This study examined artificial intelligence as a determinant of cyber security systems in deposit money banks. It discovered that artificial intelligence positively affects the cyber security system of deposit money banks in Southeast Nigeria. This suggests that an embrace and effective implementation of artificial intelligence by these banks enhances and solidifies their cyber security systems' effectiveness, acting as defence agents against cyber threats/attacks. The study also reported that artificial intelligence significantly mitigates deposit money banks' cyber security threats/attacks. This implies that effective execution of artificial intelligence in support of the cyber security system provides information on customers' behaviour and interest and helps prevent cyber threats and attacks against customers' interests. This position gives the deposit money banks the stand of attracting more customers, retaining existing ones and winning their patronage and loyalty.

5.3 Recommendations

After a critical consideration of the discussion, findings and conclusion so far, the following recommendations are made:

Deposit money banks should embrace, invest heavily in, and effectively utilise artificial intelligence to enhance and solidify their cyber security system, as doing so will generate trust and confidence in the minds of their customers, attract more customers, retain existing ones, increase patronage, and win loyalty.

Deposit money banks should train and retrain their staff/employees adequately on the knowledge, uses, applications and workings of artificial intelligence and as it relates to cyber security in banking and other financial matters, as doing so will help the workers to be on the same page in operations, enable them to detect fraud, and build a defence against cybercrimes and other financial threats/attacks.

References

1. *Adel, I.A. & A. Sara, (2019). Evaluation of telecommunications regulatory practice in the Kingdom of Bahrain: development and challenges, International Journal of Business Information Systems 31(2), 282.*

2. *Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020). Critical Cyber Security Threats: Frontline Issues Faced by Bahraini Organisations. In Implementing Computational Intelligence Techniques for Security Systems Design 210-229.*

3. *Boer, M. & Vazques J. (2017). Cyber security and financial stability: How cyber-attacks could materially impact the global financial system. Institute of International Finance Report, 1-9.*

4. *Bostrom, & Nick, (2005) "A history of trans humanist thought", Journal of Evolution and Technology, 2-21.*

5. *Caron, M. S. (2019)."The transformative effect of AI on the banking industry". Banking & Finance Law Review 34(2), 169–214.*

6. *Cidon, A., Gavish, L. & M. Perone, (2019). System and method for ai-based anti-fraud user training and protection. US Patent Application Barracuda Networks Inc,15/693,353.*

7. *Clemente, D. (2013). Cyber security and global interdependence: what is critical? : Chatham House, Royal Institute of International Affairs.*

8. *Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13-21.*

9. *Davide, S. & G. V. (2019). Houngbonon, Role of artificial intelligence in supporting development in emerging markets. International Journal Economic Development, 2(4), 191-198.*

10. *Hasham, S., Joshi, S. & Mikkelsen, D., (2019). Financial Crime and Fraud In The Age of Cyber Security. McKinsey & Company.*

11. National Science and Technology Council (2016). The National Artificial Intelligence Research and Development Strategic Plan.

12. Siddiqui, M.Z., Yadav, S. & M.S. Husain, (2018). Application of artificial intelligence in fighting against cyber crimes: A REVIEW. *International Journal of Advanced Research in Computer Science,* 9(2), 118.

13. Sindhu, J. & R. Namratha, (2019). Impact of Artificial Intelligence in chosen Indian Commercial Bank-A Cost-Benefit Analysis. Asian *Journal of Management,* 10(4), 377-384.

14. Singh, K. (2020). "Banks banking on ai". International Journal of Advanced Research in Management and Social Sciences 9(9), 1–11.

15. Soni, V. D. (2019). Role of artificial intelligence in combating cyber threats in banking. *International* Engineering *Journal for Research and Development,* 4,(1), 1-7.

16. Stamfort, Conn. (2020). Gartner Survey. Accessed in Gartner Survey Reveals 66% of Organizations Increased or Did Not Change AI Investments Since the Onset of COVID-19.

17. Vieira, A. & Sehgal A. (2018). How banks can better serve their customers through artificial techniques. In Digital marketplaces unleashed, Springer, Berlin, Heidelberg. 311-326.

18. Vishal D. S. (2019). Role of artificial intelligence in combating cyber threats in Banking, *International Engineering Journal For Research & Development*, 4(1).

19. Xie, M. (2019). Development of artificial intelligence and effects on the financial system. *Journal of Physics,* 2(2), 1-5.

20. Yazbeck, S.B., Frickenstein, J., & Medine, D. (2019). Cybersecurity in financial sector development: challenges and potential solutions for financial inclusion. *European Journal of Financial and Economic Development,* 3(6), 3-14.