KING-UK International Journal of Academic Anthology, UNITED STATES
ISSN: 2630-7230 HC, 2630-7231 SC, VOL.9 NO.1, SEPTEMBER 2025

THE ROLE OF CLOUD COMPUTING AND BLOCKCHAIN TECHNOLOGY IN PREVENTING FRAUD IN COMMERCIAL BANKS IN SOUTH-SOUTH, NIGERIA

By
NTUEN, Imoh Aniebiet,

Prof. Effiong Edet ASUQUO

And

Commy P. GODDYMKPA, PhD
Department of Business Education,
University of Uyo, Akwa Ibom state.

ABSTRACT

The study assessed the role of ***cloud computing and blockchain technology in preventing fraud in commercial banks in south-south Nigeria.*** *Descriptive survey research design was used. The study location in terms of research area was south-south Nigeria. The study population is 956 senior staff in registered commercial banks within the regions of South-South, Nigeria. This consisted of managers, accountants and cash officers of the 32 active commercial banks in South-South of Nigeria (Small and Middle-Scale Enterprise Development Agency in Nigeria (SMEDAN 2024). The study obtained a sample of 282 respondents from the overall population. The researcher developed a structured instrument titled: Emerging Technologies and Prevention of Fraud Occurrence (ETPFQ) for data collection. Face and content validation was used. The analysis of the data obtained was done in Cronbach Alpha where it presented a coefficient of 0.85.The research questions were addressed through the application of mean statistics, whereas the null hypotheses were examined with Analysis of Variance (ANOVA) at the .05 significance level.In conclusion, cloud computing and blockchain technology play a pivotal role in strengthening fraud prevention mechanisms in commercial banks within South-South Nigeria.The study recommended that commercial banks can strategically use cloud computing to enhance efficiency, agility and competitiveness.*

KEYWORDS: Cloud Computing, Blockchain Technology, Fraud, Commercial Banks, South-South, Nigeria

INTRODUCTION

Emerging technologies bestow vital opportunities on businesses to elevate their customers' experience and secure a competitive advantage. Amid the technological revolution, reliance on emerging technologies has intensified over the last few years. Brigitte et al (2015) maintain that these technologies allow firms to extend their outreach at only a fraction of the cost of traditional channels while delivering greater convenience to clients and more effectively achieving their organisational objectives. Among the emerging technologies are cloud computing and blockchain technology, Such technologies can assist organisations

in overcoming problems such as risk management, customer satisfaction, upgraded product offerings, and elevated operating costs, among others.

Cloud computing involves employing a network of remote servers residing in the internet to store, oversee, and handle data instead of depending on an onsite server or personal computer. Cloud computing, in essence, denotes the provision of computing services online—for example, databases and related solutions. According to Licklider (2023), the cloud supplies greater flexibility and reliability, boosts performance and efficiency, and also costs less to manage inflammation-related technology. Moreover, Licklider maintained that it further boosts innovation by enabling organisations to reach market sooner and embed artificial intelligence and machine learning use cases into their strategies. Nevertheless, Weinman (2011) noted that data loss, or data leakage, constitutes the most frequent cloud security hazard associated with cloud computing. In Weinman's view, data loss references situations in which data is rendered corrupt, deleted, or rendered unreadable for a user, application, or software. According to Douglas (2019), some measures for surmounting cloud computing challenges include selecting the most suitable cloud service model, enforcing a comprehensive cloud security strategy, minimising cloud spending, overseeing cloud performance, and building steadily on cloud expertise to enable blockchain technology to operate effectively. Cloud computing will operate seamlessly only when blockchain is incorporated into the mix.

Blockchain technology constitutes a sophisticated database architecture that makes transparent data sharing possible across a business network. Referred to as Distributed Ledger Technology (DLT), blockchain is a reliable, decentralised ledger that both securely stores and validates transactions. It operates as a shared ledger that permits every network participant to access it. Satoshi (2018) contended that blockchain operates with an authorised participant entering each transaction. The transaction is first verified and subsequently recorded within a block. The block is dispersed to all the nodes in the network. Conduction nodes confirm the transaction and appended the block to the chain. Once the update propagates throughout the network, the transaction is thereby finalised. Blockchain may be employed to follow the movement of assets. Satoshi further maintained that blockchain can record assets such as real estate, vehicles, funds, intellectual property, patents, and copyrights. Regarding transaction logging, blockchain is capable of documenting orders, flows of payment, and accounts. With respect to facilitating transactions, blockchain can make transactions possible among parties marked by mutual distrust. With regard to diminishing risk and expenses, Masters (2018) asserted that blockchain achieves this by delivering immediate, shared, and openly observable information. According to Kindergan (2017), most blockchains function autonomously, upholding distinct rules and data structures. Insufficient interoperability might obstruct effortless sharing of data among blockchains and thus trigger regulatory complications. Thompson (2018) contends that these challenges can be remedied through sound finance, sound understanding of customer activity, the capital market, robust regulatory compliance and supervision. Blockchain enables financial organisations to carry out international financial transactions more swiftly and at lower costs than is possible with current platforms such as Swift. The approach would be even more effective if data analytics were considered.

Statement of Problem

Dependence on emerging technologies has intensified over the past few years, propelled not only by the expansion of the banking system but also by the technological revolution it has unleashed. These technologies enhance banking operations and help in providing safeguards in its banking activities. However, fraud remains a significant challenge in the banking sector, with commercial banks facing increasing threats from cyber fraud, Automatic Teller Machine fraud, phishing, insider threats, identity theft, and unauthorisedaccess to financial systems. These fraudulent happenings have led to momentous financial losses, declining public confidence in banking institutions, and interrupted financial activities. In spite of the regulatory measures, security protocols employed by financial institutions, fraudsters remain resolute in developing classy techniques to bypass fraud detection mechanisms.In response to these challenges, commercial banks have begun embracing emerging technologies—among them Artificial Intelligence (AI), Machine Learning (ML), Blockchain.

Research Objective

1. The extent to which the use of cloud computing prevents fraud occurrence in commercial banks in South-South, Nigeria.
2. The extent to which the use of blockchain technology prevents fraud occurrence in commercial banks in South-South, Nigeria.

Research Question

The following research questions guided the study:

i. To what extent does the use of cloud computing prevent fraud occurrence commercial banks in South-South, Nigeria?
ii. To what extent does the use of blockchain prevent fraud occurrence in commercial banks in South-South, Nigeria?

Research Hypothesis

The following hypotheses were formulated and tested at 0.5 level of significance:

Ho_1: There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks in South-South, Nigeria.

Ho_2: There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of blockchaintechnologyprevents fraud occurrence in commercial banks in South-South, Nigeria.

Conceptual Review

Emerging Technologies

Any application of scientific knowledge for practical purposes, often involving the creation and utilisation of tools, equipment, and systems to address challenges and enhance human life is termed technology. Technology is a prefix of the Greek language-"techne" that means art and craft and logos which means word and speech. The term was initially applied on applied arts. The history of technology is the history of the invention of tools and techniques by humans. Technology; according to Sinan (2022) encompasses technologies that vary in their complexity levels starting with mere stonework tools all the way to advanced genetic engineering and information technology that has come up since the 1980s. However, it is currently also employed to explain development and changes that occur to a surrounding

environment. It also refers to technology or the use of scientific discoveries in light of practical purposes of human life or in an expression that is often used, to change and modify the human environment.

Xuan (2021) described technology as machine and equipment that has been created based on the use of scientific knowledge. By this, Xuan will say that it will lower the capability of the industry to invest in new technology. At least, according to the opinion of Feng (2018), it is the field of knowledge hairing on engineering or applied sciences. Feng also hypothesised that by modernising the core banking systems, banks are able to give smooth and customised customer experiences. Consequently, alongside that, Zang (2021) indicated the advancement of technologies, which made digital interaction, i.e. real-time account access, recommendations, and individual product suggestions, and expedited processing of transactions more satisfying to the customers and loyal to the company. Xuan (2018) claims that one of the most impressive effects of technology on the banking industry is the process of digitalisation. Since the introduction of the online and mobile banking services, the customers are now able to have access to a very large variety of banking services right in the comfort of their smartphones or computers. Xuan (2021) also claimed that financial technology is used to provide financial services to more people and even underserved communities as well as those who have a lower-access level to traditional financial services.

The author of the paper Zang (2021) expressed an opinion by noting that the introduction of online and mobile banking has become a possibility to provide a vast number of banking services to customers with their smartphone or computer. Besides leading to efficiency and speed in banking processes, this transformation as envisioned by Zang has led to an improvement in the experience of customers as a whole because the banking institutions can use computing, artificial intelligence, and use of information into data analytics to revise their primary banking systems to provide the necessary support to customers and remain relevant in the market. Zang also added that financial technology solutions are automating processes and playing roles in the reduction of costs as well as the increase in speed and accuracy in the financial transactions. According to Abaenewe (2019), one of the greatest technological effect on the banking sector is the transition to digitalisation. Following the introduction of online and mobile banking, Abaenewe further said that clients can now enjoy diverse services offered by banks through their smartphones or their computer using the internet. Nevertheless, some of the main drawbacks of e-banking and their potential influence on the customers as postulated by Eyitayo et al. (2013) are: Technical issues, absence of personal relationships, internet fraud, inability to provide numerous services, how to consider the risk of banks, technology risk, cybersecurity, risk of failing to comply with the regulations of data protection, risk of using legacy system among others. As the banks come up with comprehensive strategies on how to handle the financial risks, Eyitayo indicated further that the banks might not realize the risk that comes with technology.

These issues as per Francis (2017) should be dealt with by commercial banks. It is their responsibility to make sure that their systems are inoculated and incapacitated against data leak, phishing attacks and other attacks. Besides that, Francis added that this would need an investment in high-end cybersecurity systems like a multi-factor authentication, encryption, real-time monitoring network traffic and investing in compliance technology. Chukwuebuka et al. (2022) believe that automation tools must guide and in some way make

sure that all the complicated regulatory demands are met. Regarding the development of scalable systems, make sure that institution has flexible processes and personnel to ensure that it maintains compliance with the emerging standards without overloading the available resources.

Fraud Occurrence

Fraud is the act of deceiving someone to gain a personal or financial advantage. It can involve the use of false information, concealment of facts, or other unethical means. Fraud is an offence. Fraud is any practice or practice, in which deception is used, with the objective to attain a benefit. According to Muritala et al. (2020) the misrepresentation of the truth leads fraud to be a crime when it is a knowing misrepresentation. According to the belief held by Talmar, (2021) fraud is a deliberate information deception. Muritala et al. went ahead and gave the examples of business fraud to encompass theft, bribery, insider trading and false financial information. These activities as described by Muyanja are done to trick stakeholders, foreign money exchange rip-offs, counterfeit cashier's checks, fake debts, home repair rip-offs, business opportunities or employment scam to mention a few.

Examples of fraud as listed by Tracy (2012) include embezzlement, forgery, financial fraud, misuse of resources, unauthorised payments, conflict of interest, scamming among others. In terms of embezzlement, it means stealing money or property from an organisation or person. In terms of forgery, altering or falsifying of documents. In terms of financial fraud, misrepresenting financial information to gain money. In terms of misuse of resources, using an organisation's resources for personal gain. In terms of unauthorised payments, it means receiving payment for goods or services that were not provided. Conflict of interest means violating ethical rules or engaging in a conflict of interest. Scamming means tricking someone into donating money or participating in an activity.

These frauds according to Tracy are committed by individuals, employees, contractors among others. Individuals can commit fraud to gain personal advantage. Employees can commit fraud to gain financial benefits or money and contractors can commit fraud by claiming for services they did not provide. Anyone can be a victim of fraud. Anyone who is deceived by another person or organisation. Anyone who has their money or property taken by another person or organisation. To this effect, Zadia (2021) maintained that the occurrence of fraud is a measure put in place to ensure that fraudulent transactions or banking behavior are identified and such acts are intercepted before they result in financial and reputational consequences to both the customers and the financial institutions. Besides that, fraud occurrence as described by Martin (2021) is the polices, functions, and processes by a firm that prevent the occurrence of fraud. Martin added that there is no fool proof strategy when it comes to fraud occurrence but companies can work towards preventing the kind of fraud they are most prone to. This in the words of Martin will make them use their resources optimally. To achieve this effectively, Steven argued that they can have frequent risk testing to make sure that they use sound risks in their model.

Cloud Computing and Prevention of Fraud Occurrence

Cloud computing entails using multiple internet-based servers to store, handle, and process data, as opposed to using a local server or a personal computer. The cloud constitutes servers housed within data centres across the globe. Benson (2024) argued that, since cloud-

based workloads run on data centre servers rather than locally on the user device, individuals can access consistent files and applications from virtually any device. Hence, Benson (2024) noted that if a user's old phone fails, they can still log in to their Instagram account on a new device and find all their photos, videos, and conversation history waiting for them on the old account. Benson similarly explained that cloud email services such as Gmail or Microsoft office 365 function the same way, and that the same holds true for cloud storage services such as Dropbox or Google Drive. Benson contends that shifting to the cloud helps companies cut expenses while also enhancing users' convenience.

Krishnan (2021) contended that, besides greater flexibility and reliability, the cloud offers enhanced performance and efficiency and helps reduce IT costs. It likewise advances innovation, letting companies shorten time-to-market and weave artificial intelligence and machine learning use cases into their strategic frameworks. Furthermore, Krishnan argued that the cloud enables financial institutions to keep customer data in centralised centres and to adjust the scale of the services they subscribe to whenever necessary. Ezenwoke (2023) contends that cloud computing delivers heightened flexibility, greater efficiency and greater strategic value than traditional on-premises information technology infrastructure. Benefield et al. (2018) observe that financial institutions keep their customer data stored in central facilities and adjust the services they have subscribed to according to their evolving needs. As Benefield et al. argue, commercial banks and other financial institutions can sidestep the costs of acquiring, sustaining, and upgrading physical servers. Such services can be offered free of charge or charged on an on-demand basis, letting customers incur charges exclusively for the CPU cycles, storage, or bandwidth they consume. By adopting a pay-per-use pricing scheme, cloud computing allows financial institutions to curtail their storage expenses instead of incurring considerable upfront costs. Qi (2010) maintained that it empowers banks to address fully customers' needs and expectations by enhancing connectivity, leveraging data-driven insights, boosting operational efficiency, and strengthening risk management. QI added that financial institutions are spared from the expenses involved in buying, maintaining, and upgrading physical servers. Blessing contends that under the pay-as-you-go model, firms reap significant cost savings by only having to pay for the services they consumption.

Guhen (2018) suggested that implementation of cloud computing in commercial banks and financial services enables the institutions to cut expenses associated with owning and maintaining on-premises infrastructure and data centres. Guhen likewise contended that cloud computing users and companies relinquish the responsibility of overseeing physical servers directly and equally forgo the task of operating software applications on their in-house machines. According to Douglas (2019), deploying cloud computing solutions within the banking industry equips institutions with heightened scalability and flexibility, cuts operational costs, bolsters business continuity, upgrades data security and fraud detection, decreases expenses, reinforces defences, meets regulatory requirements and enhances customer relationship management (CRM). Even after migrating to the cloud, Douglas still contended that commercial banks no longer have to maintain on-premises servers, the cooling systems that come with them, and the attendant infrastructure.

According to the pay-as-you-go model advanced by Satoshi (2018), firms are billed only for the resources they consume, enabling them to realise significant cost savings. As per Kratzke's (2022) perspectives, cloud computing falls into four distinct categories—public

cloud, private cloud, community cloud, and hybrid cloud. Among these deployment models, Mckenzie (2017) cites four principal services—infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), and serverless computing along with its scalability and flexibility. Such a framework can function successfully only if public cloud is incorporated.

Blockchain Technology and Prevention of Fraud Occurrence

Blockchain technology is defined as a technology that utilises a chain of blocks to securely store and manage data in a decentralised manner. According to the postulation of Masters (2018) blockchain is data blocks interlocked in a chain that cannot be edited. This data as per Monika is cached in an open-source decentralised network, where the data contains on each block is verifiable by all the involved computers. The postulated version of blockchain (Thompson, 2018) considerably lowers the cost of overhead and transaction, and lessens or eschews third parties or middle arrangers in establishing the verity of the transaction. According to Thomas, there are four principal kinds of blockchain networks that include; public blockchains, private blockchains, consortium blockchains as well as hybrid blockchains. As postulated by Thompson, a public blockchain is a decentralised network that can be read and written by anyone without seeking the permission of the central authority; there is no Central Authority which controls what and how communication occurs amongst the people. According to Thomas, they use an open-source framework, and this makes them transparent and secure following the cryptographic principles. Public blockchain also included programs located on the blockchain system and which automatically perform under the condition of their needs. Thomas also asserted that they run if-then checks to ensure that transactions can be carried out without any fear. As an example, a logistics company can possess a smart contract that automatically executes the payment after delivery of goods has been reached at the port. Kindergan (2017) further noted that blockchain eradicates fearful or redundant transactions through time stamping of any transaction in turns.

Kindergan (2017) argued that it was possible to make transactions without involving intermediaries because smart contracts can automatically impose suitable responses to the designated stakeholders. Thompson (2018) claimed that the advantages of blockchain included the growth of trust, security and transparency across member organisations by enhancing the traceability of information and data shared across a business network, and the potential of cost savings as a result of new efficiencies. In addition to the statement on advance traceability, Thompson (2018) claimed that blockchain would also allow managing inventory efficiently since it would allow real-time insights into the levels of inventory to optimise replenishment and consequently minimise stockouts. Thompson (2018) supported by saying that constant monitoring is one of the most important elements that commercial banks and other financial institutions should take into consideration when it comes to preventing fraud. In an op-ed article by Oseni (2016), she opined that such form of monitoring could be done on a cloud-based platform and this would enable them to detect and counter suspicious activities in real time.

Masters (2018) also highlighted that blockchain enables parties to transact among themselves without any centralised transaction processors to the extent that the transaction could be faster which means the cost of transactions could be lower.

Blockchain is a peer-to-peer network, according to the postulation of Alderson (2017), which means that several computers, or nodes, collaborate in order to validate and confirm the transaction. This technology as it has been argued by Stafinda could transform fraud detection and their occurrence through transparency, immutability and security. The same is possible due to the implementation of blockchain technology which, according to findings by Evan-Greenwood (2016), allows one to monitor the transactions real-time using instant access to the history of transactions within the network. This on the part of Evan-Greenwood allows organisations to monitor and examine transaction in real-time thus enabling the organisations to apprehend and purge fraud as it happens. A private blockchain according to the postulation by Alderson (2017) is a decentralised ledger which is accessible to only a group of specific individuals or organisations. Alderson continued to say that it contains only one operator/entity who can decide who can access the network, see the information and make data on blockchain. Alderson insisted through the application of the private blockchain, people will be able to be in greater control over their personal information, and they will be less likely to have cases of identity theft.

Methodology

Descriptive survey research design was used. The study location in terms of research area was south-south Nigeria. The study population is 956 senior staff in registered commercial banks within the regions of South-South, Nigeria. This consisted of managers, accountants and cash officers of the 32 active commercial banks in South-South of Nigeria (Small and Middle-Scale Enterprise Development Agency in Nigeria (SMEDAN 2024). The study obtained a sample of 282 respondents from the overall population. The researcher developed a structured instrument titled: Emerging Technologies and Prevention of Fraud Occurrence (ETPFQ) for data collection. Face and content validation was used. The analysis of the data obtained was done in Cronbach Alpha where it presented a coefficient of 0.85.The research questions were addressed through the application of mean statistics, whereas the null hypotheses were examined with Analysis of Variance (ANOVA) at the .05 significance level.

Result and Discussion

Research Question One

To what extent does the use of cloud computing prevent fraud occurrence commercial banks in South-South, Nigeria?

Table 1: Summary of mean on theextent of use of cloud computing to prevent fraud occurrence in commercial banks N=282

S/N	CLOUD COMPUTING	Mean	Std. Dev.	Remark
1.	Allowing for efficient resource utilisation	2.15	1.21	LE*
2.	Increasing scalability to meet demands	2.12	1.18	LE
3.	Implementing robust security measures	2.16	1.21	LE
4.	Having good networking storage	2.22	1.30	LE
5.	Having different service models	2.14	1.28	LE
6.	Having good storage capacity	2.15	1.21	LE
7.	Providing flexibility to changing workload	2.24	1.30	LE
8.	Protecting infrastructure	2.24	1.34	LE
9.	Having access control	2.30	1.37	LE
10.	Being able to manage data	2.25	1.36	LE

Cluster Mean	**2.20**	**1.28**	**LE**

*LE: Little Extent. Source: Researcher's field computation

Table 1 gives a summary of the mean and item analysis on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks. The result shows that the mean range is 2.12 -2.25. The standard deviation ranges from 1.18 -136, indicating that the responses are close and not too dispersed from each other. The result shows that all the items have their mean within 1.50 – 2.49 indicating that there is a little extent to which the use of cloud computing prevents fraud occurrence. The cluster mean of the responses is 2.20. This indicates that there is a little extent to which the use of cloud computing prevents fraud occurrence in commercial banks in South-South, Nigeria.

Research Question Two

To what extent does the use of blockchain prevent fraud occurrence in commercial banks in South-South, Nigeria?

Table 2:Summary of mean on the extent of use of block chain to prevent fraud occurrence in commercial banks. N=282

S/N	BLOCKCHAIN	Mean	Std. Dev.	Remark
1.	Having a distributed ledger	3.35	0.77	GE*
2.	Using cryptography to secure blockchain	3.26	0.86	GE
3.	Using consensus mechanisms for the validation of transactions	3.27	0.93	GE
4.	Laying blocks as the foundational unit of information	3.39	1.00	GE
5.	Having nodes in blockchain network	3.37	0.95	GE
6.	Using smart contracts as vital components	3.30	0.88	GE
7.	Having transactions that cannot be edited	3.55	0.74	VGE**
8.	Having transactions that are only stored in ledger	3.56	0.86	VGE
9.	Having a decentralised model to communicate between participants	3.66	0.81	VGE
10.	Ensuring the entire system is full tolerant	3.61	0.81	VGE
	Cluster Mean	**3.43**	**0.86**	**GE**

*GE- Great Extent; **VGE- Very Great Extent. Source: Researcher's field computation

Table 2 gives a summary of the mean and item analysis on the extent to which the use of blockchain prevents fraud occurrence in commercial banks. The result shows that the mean range is 3.26-3.66. The standard deviation ranges from 0.74-1.00, indicating that the responses are close and not too dispersed from each other. The result shows that all the items have mean within 2.50-3.49 indicating that there is a great extent to which the use of blockchainpreventsfraudoccurrence. The cluster means of the responses is 3.43. This indicates that there is a great extent to which the use of blockchainprevents fraud occurrence in commercial banks in South-South, Nigeria.

Hypothesis Testing

Research Hypothesis 1

There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks in South-South, Nigeria.

Table 3a: Summary of Analysis of Variance (ANOVA) test for significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks

		Sum of Squares	df	Mean Square	F	Sig.
Allowing for efficient resource utilization	Between Groups	84.843	2	42.422	36.350	.001
	Within Groups	325.600	279	1.167		
	Total	410.443	281			
Increasing scalability to meet demands	Between Groups	49.813	2	24.906	20.240	.001
	Within Groups	343.325	279	1.231		
	Total	393.138	281			
Implementing robust security measures	Between Groups	56.100	2	28.050	22.125	.001
	Within Groups	353.719	279	1.268		
	Total	409.819	281			
Having good networking storage	Between Groups	36.636	2	18.318	11.690	.001
	Within Groups	437.169	279	1.567		
	Total	473.805	281			
Having different service models	Between Groups	79.597	2	39.799	29.012	.001
	Within Groups	382.729	279	1.372		
	Total	462.326	281			
Having good storage capacity	Between Groups	65.381	2	32.690	26.181	.001
	Within Groups	348.364	279	1.249		
	Total	413.745	281			
Providing flexibility to changing workload	Between Groups	100.714	2	50.357	37.881	.001
	Within Groups	370.889	279	1.329		
	Total	471.603	281			
Protecting infrastructure	Between Groups	83.898	2	41.949	27.720	.001
	Within Groups	422.219	279	1.513		
	Total	506.117	281			
Having access control	Between Groups	109.728	2	54.864	36.510	.001
	Within Groups	419.251	279	1.503		
	Total	528.979	281			
Being able to manage data	Between Groups	40.801	2	20.400	11.899	.001
	Within Groups	478.323	279	1.714		
	Total	519.124	281			
Average						**.001**

Table 3a presents the summary of the analysis of variance test for significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks. The result indicates that the probability values (p-values) for all the items as responded to by managers, accountants and cash officers are significant at $p < .05$. The average p-value value is .001. Since $p < .05_{.001}$, the

result is statistically significant. Thus, there is a significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks in South-South, Nigeria. Based on the observed difference, a post hoc test is carried out to determine the direction of the difference.

Table 3b: Scheffe's Test for direction of significance

(I) Experts	(J) Experts	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Managers	Accountants	-2.18750*	.27007	.001	-2.8521	-1.5229
	Cash officers	-.68463*	.20451	.004	-1.1879	-.1814
Accountants	Managers	2.18750*	.27007	.001	1.5229	2.8521
	Cash officers	1.50287*	.20451	.221	.9996	2.0061
Cash officers	Managers	.68463*	.20451	.004	.1814	1.1879
	Accountants	-1.50287*	.20451	.221	-2.0061	-.9996

*. The mean difference is significant at the 0.05 level

Table 3b presents the summary of the post hoc test. The result shows probability values of .001 and .004 for managers' views as against cash officers and accountants, indicating a significant difference between managers' views of the use of cloud computing for prevention of fraud occurrence differ significantly from those of accountants and cash officers. The result also showed no significant difference in the responses of accountants and cash officers. Thus, the significance lies in the managers' responses. Thus, managers differ significantly from accountants and cash officers on the extent to which the use of cloud computing prevents fraud occurrence in commercial banks in South-South, Nigeria.

Research Hypothesis 2

There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of blockchain technology prevents fraud occurrence in commercial banks in South-South, Nigeria.

Table 4: Summary of ANOVA test for significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of blockchainprevents fraud occurrence in commercial banks

		Sum of Squares	df	Mean Square	F	Sig.
Having a distributed ledger	Between Groups	17.836	2	8.918	16.575	.101
	Within Groups	150.108	279	.538		
	Total	167.943	281			
Using cryptography to secure blockchain	Between Groups	3.830	2	1.915	2.635	.074
	Within Groups	202.752	279	.727		
	Total	206.582	281			
Using consensus mechanisms for the validation of transactions	Between Groups	8.807	2	4.404	5.235	.106
	Within Groups	234.710	279	.841		
	Total	243.518	281			
Laying blocks as the foundational unit of information	Between Groups	7.289	2	3.644	3.687	.126
	Within Groups	275.804	279	.989		
	Total	283.092	281			
Having nodes in blockchain network	Between Groups	8.387	2	4.193	4.770	.079
	Within Groups	245.259	279	.879		
	Total	253.645	281			
Using smart contracts as vital components	Between Groups	12.449	2	6.225	8.409	.101
	Within Groups	206.529	279	.740		
	Total	218.979	281			
Having transactions that cannot be edited	Between Groups	14.418	2	7.209	14.420	.092
	Within Groups	139.483	279	.500		
	Total	153.901	281			
Having transactions that are only stored in ledger	Between Groups	7.498	2	3.749	5.179	.160
	Within Groups	201.977	279	.724		
	Total	209.475	281			
Having a decentralised model to communicate between participants	Between Groups	28.852	2	14.426	26.056	.231
	Within Groups	154.468	279	.554		
	Total	183.319	281			
Ensuring the entire system is full tolerant	Between Groups	1.321	2	.660	1.014	.364
	Within Groups	181.772	279	.652		

	Total	183.092	281
			0.143

Table 4. presents the summary of the analysis of variance test for significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of blockchaintoprevent fraud occurrence in commercial banks. The result indicates that the probability values (p-values) for all the items as responded to by managers, accountants, and cash officers are higher than the alpha level of .05 (p> .05). This indicates that the result is statistically not significant. The average p-value is .143. Since p>.05 .143, the result is statistically not significant. Thus, there is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of blockchainprevents fraud occurrence in commercial banks in South-South, Nigeria.

Conclusion

In conclusion, cloud computing and blockchain technology play a pivotal role in strengthening fraud prevention mechanisms in commercial banks within South-South Nigeria. Cloud computing enhances data security through real-time monitoring, advanced encryption, and efficient storage systems, thereby reducing vulnerabilities associated with traditional banking infrastructure. Similarly, blockchain technology provides transparency, immutability, and decentralized transaction validation, making it increasingly difficult for fraudulent activities to go undetected. Although challenges such as infrastructural limitations, regulatory gaps, and high implementation costs remain, the combined adoption of these technologies offers commercial banks a sustainable pathway toward improved fraud detection, enhanced trust, and greater operational resilience in the region.

Recommendations

i) The commercial banks can strategically use cloud computing to enhance efficiency, agility and competitiveness.

ii) Commercial banks ought to study and effectively use blockchain in support of their operations, security, transparency and efficiency of operations.

iii) Commercial banks are advised to adopt strong data encryption mechanism or even a strong data encryption so that they not only protect the information of the customers but can also meet the regulations such as and other regulations.

REFERENCES

Abaenewe, Z. C., Ogbulu, O. M. and Ndugbu, M. O. (2013). Electronic banking and bank performance in Nigeria West African. *Journal of Industrial & Academic Research*, 6(1): 171-187.

Alderson, D. (2017). *Organized Complexity in Network Insights and Opportunities*. (Online). Available: https://internationalc2institute.org/2017-plenary. Accessed 5 September, 2018.

Benefield, B., Herford. S. and Thomas, K. (2018). *Blockchain - What to Consider when Choosing a Blockchain Framework.[Online]*. Available: https://www.researchgate.net/profile/James_Herford2/publication/326635534_Blockchain-_What_toMB_Consider_when_Choosing_a_Blockchain_Frameworki/links/5b5a1fbaaca272a2d66cc327/Blockchain-What-to-Consider-when-Choosing-a-Blockchain-Frameworki?origin=searchReac. Accessed July 2018.

Benson, C. (2024). *Blockchain Security: What Keeps your Transaction Data Safe?*. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/. (Accessed 2 February 2024).

Brigitte, M., Chiu, V. and Qi, L. (2015). Emerging technologies and research in accounting. *Research Journal of Information Technology*, 12(1): 25-41. Doi:150807112321006:10.2308/jet-a-51245.

Chukwuebuka, B., Azolibe I., Jisike J. O. and Ogochukwu, V. O. (2022). *Technology-based Banking and Bank Deposit: The Nigerian Commercial Banks' Experience*. https://doi.org/10.1080/20421338.2021.2015164.

Douglas, M. (2019). *Blogging Software as a Service*. Retrieved 5 March, 2015 from https://www.compendium.com/blog/social-media-domination/blogging-software-as-a-service.

Eyitayo F. A., Oluwafemi, C. O. and Yolanda N. N. (2024). Influence of technological usage on customer service and customer satisfaction in the banking sector. *Journal of Applied Science and Technology*, 8(4):1979-1985. DOI: 10.55214/25768484.v8i4.1572.

Ezenwoke, J. M. (2023). *Is Bitcoin Really Un-Tethered?*Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066. (Accessed 16 March 2022).

Feng, M. (2018). Analysis of innovation development trend of financial technology and commercial bank. *Industry Innovation Research*, 2(3): 10-17.

Francis, I. (2021). Impact of information technology on Nigeria banking industry: a case study of Skye Bank. *International Journal of Computing Sciences Research*, 1(1): 25-35.

Guhen, H. V. (2018). Exit-chart aided quantum code design improves the normalised throughput of realistic quantum devices. *IEEE Access*, 4(7), 94–110.

Kindergan, A. (2017). *Forget Bitcoin but Remember Blockchain*. (Online). Available: https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/forget-bitcoin-but-remember-blockchain-201702/html. (Accessed 27 August, 2018).

Krishnan B. (2011). *Hybrid Clouds*. Retrieved 20 March, 2013. from https://la.trendmicro.com/media/wp/hybrid -clouds-whitepaper-en.pdf.

Licklider, G. (2023). *The Birth of Cloud Computing*. United States of America. Brand with advertising.

Masters, C. (2018). *Can Blockchain Displace SWFT Banking Transfer*? (Online). Available: https://crytovest.com/news/can-blockchain-displace-swft- banking. transfer/Accessed 27 August, 2018.

Mckenzie, F. (2017). *The Bitcoin Bubble and the Future of Currency*. Available: https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb. (Accessed 10 January 2018).

Muritala, A, T. and Muftau, A. I. (2020). Fraud and bank performance in Nigeria – var granger causality analysis. *Financial Internet Quarterly*, 16(1):20-26. DOI: 10.2478/fiqf-2020-0003.

Oseni, E. (2016). *Across the Counter Frauds in the Banking Industry and Evaluation of Some of the Available Control*. Journal of Innovative Technology, 7 (11): 116-132.

Qi, Z. (2010). Cloud computing: State-of-the-art and research applications. *International Journal of Science,* 1(1): 7-18.

Satoshi, N. (2017). *Why is the Community so Negative TowardsBlockchain Technology* (online). Available: https://news.combination.com/item?:d=13420777 (Accessed 29 August, 2018.

Sinan, E. (2022). Emerging Technologies: Value Creation for Sustainable Development. Springer, Nigeria.

Tarmar, M. (2021). *Applied Craptography: Bitcoin and Other Cryptocurrencies*. Available: http://gamescrafters.berkeley.edu/~cs161/fa16/slides/lec_bitcoin.pdf. (Accessed 27 August 2022).

Thompson, L. (2018). *Beijing Tightens it's Grip on DomesticBlockchain networks*. Asia. Times holding limited. (Online). Available: https://www. a times.com/article/beijing-tightens-its-grp-on-domestic-block-netwwork/. Accessed 26 Oct. 2018).

Tracy, O. (2012). *The Story of the Blockchain*. Triple Smoke Stack, New York.

Weinman, J. (2011). *Network Implications of Cloud Computing*. Springers Publishers, Australia.

Xuan, G. (2022). A study on the impact of commercial banks' digital transformation on ESG performance—based on empirical evidence from listed banks in China. *Academic Journal of Business and Management* 5(23):119-124. DOI: 10.25236/AJBM.2023.052318.

Zadia, V. L. (2021). *To Blockchain or Not to Blockchain: That is the Question*. [Online]. Zang, L. (2021). Application of financial technology innovation in commercial banks: A case study of bank of China. *International Journal of New Developments in Engineering and Society*, 5(3): 47-53, DOI: 10.25236/IJNDES.2021.050306.