WORLD ATLAS INTERNATIONAL JOURNAL OF EDUCATION & MANAGEMENT
VOL 8 NO 1, OCTOBER 2025, NEW YORK CITY. *ISSN: 2667-1069*

DATA ENCRYPTION AND AUTHENTICATION AS FRAUD PREVENTION MECHANISMS IN COMMERCIAL BANKS IN SOUTH-SOUTH, NIGERIA

By

Samuel David UDO, PhD

And

NTUEN, Imoh Aniebiet
Department of Business Education,
University of Uyo, Akwa Ibom state.

ABSTRACT

The study assessed the Data Encryption and Authentication as Fraud Prevention Mechanisms in Commercial Banks in South-South, Nigeria. A 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 sample consists of 32 managers, 32 accountants, and 218 cash officers. Taro Yamane's formula will be applied to choose the sample. The researcher developed a structured instrument titled Emerging Technologies and Prevention of Fraud Occurrence (ETPFQ) for data collection. Face and content validation were used. The analysis of the data obtained was done in Cronbach's 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. The study showed that there is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of data encryption and authentication prevents fraud occurrence in commercial banks in South-South, Nigeria. One of the recommendations made was that commercial banks are advised to adopt a 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 other regulations.

Keywords: Data Encryption, Authentication, Fraud Prevention Mechanisms 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, blockchain technology, real-time monitoring, mobile technologies, data encryption, quantum computing, and

artificial intelligence. Such technologies can assist organisations in overcoming problems such as risk management, customer satisfaction, upgraded product offerings, and elevated operating costs, among others.

Data encryption entails capturing information and translating it into a form that, ideally, only authorised users can revert to its original The procedure transforms the original formulation of the information—plaintext—into an alternative manifestation called ciphertext. Through data encryption, data is transformed from its readable plaintext form into a gibberish format, ciphertext. Leonard (2019) commented that only with cryptographic keys in hand can users or processes access encrypted information for processing. Leonard remarked that the decryption key is a secret and should, therefore, be safeguarded against unauthorised access. Leonard notes that firms employing encryption on financial records instate a formidable shield that deters malicious actors from making unauthorised attempts at access or data breaches. Consequently, Frankfurt contends that encryption curtails fraudulent behaviour and financial losses as well. In addition, Ron (2020) underscored that the use of encryption serves to foster the creation of robust disaster-recovery systems.

Authentication is the verification of an assertion, for example, confirming the identity of a computer system user. In contrast with identification—the process of signifying a person or thing's identity—authentication entails validating that very same identity. Auth… Further techniques comprise token-based authentication, certificate-based authentication, and single sign-on (SSO). Another emerging authentication approach depends on password-less verification and employs substitute methods such as security keys or one-time codes.

Emerging technologies have dominated the agenda of deliberations within the financial sector. Such occurrence is attributed to fraud, misappropriation of funds, pilfering, and other similar offences. Commercial banks are exposed to a variety of fraud threats, ranging from external fraud to internal, and it is the former that is more frequently observed. Some of the most prevalent forms of fraud entail card mishaps, check fraud, account takeover, identity theft, and investment swindles. Financial institutions are likewise susceptible to cyber threats such as phishing or SIM swapping, capable of granting unauthorised access and resulting in financial losses. Consequently, a number of commercial banks have collapsed. For instance, the central bank of Nigeria closed Merchantile Bank because it had failed to remedy severe undercapitalisation, weak corporate governance, and insolvency effects that jeopardised the interests of depositors.

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 unauthorised access 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, Big Data encryption, Biometric Authentication, and Cloud Computing—so as to sharpen fraud detection and curb occurrences. These technologies provide predictive capabilities that can enable banks to scrutinise a bulk of financial transactions, detect irregularities, and recognise suspicious patterns before fraudulent activities occur.

RESEARCH OBJECTIVE

1. The extent to which the use of data encryption prevents fraud occurrence in commercial banks in South-South, Nigeria.
2. The extent to which the use of authentication prevents fraud occurrence in commercial banks in South-South, Nigeria.

RESEARCH QUESTION

1. To what extent does the use of data encryption prevent fraud occurrence in commercial banks in South-South, Nigeria?
2. To what extent does the use of authentication prevent fraud occurrence in commercial banks in South-South, Nigeria?

Research Hypothesis

1. Ho_3: There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of data encryption prevents fraud occurrence in commercial banks in South-South, Nigeria.
2. Ho_4: There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of authentication prevents fraud occurrence in commercial banks in South-South, Nigeria.

CONCEPTUAL REVIEW

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 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 scams, 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 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 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 behaviour 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 foolproof 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.

DATA ENCRYPTION AND PREVENTION OF FRAUD OCCURRENCE

Encryption is the process of altering information in a manner that only authorised entities are supposed to decipher. The idea of encryption, as explained by Jacob (2023), is a method of garbling information in a manner that only authorised persons can decipher the data. Technically, Jacob also stated that it involves the transformation of plain text that can be read by a human being to an unintelligible text, otherwise referred to as ciphertext. Shamir (2017) asserts that data encryption involves putting data, which is in plain text, into an indecipherable encoded format that users and processes, such as Siegel, can then only read and process after decryption. On the one hand, Ezeofor *et al.,* (2014) assumed that the decryption key is confidential, and hence they should guard it against unauthorised use. Encryption, according to the view of Sidney et al. (2022), offers a means to scramble information in a manner that only authorised parties can interpret. Encryption of financial information, according to Sidney, allows organisations to establish an effective obstacle that would not tempt the malicious entities to engage in unauthorised access or data leakage. This further results in a reduction of fraud and reduces losses. In addition, Ezeofor et al. (2014) corroborated that the aspect of data encryption enhances the creation of robust disaster recovery as well as mitigation against risks in the presence of various forms of natural disasters.

Banks must employ a 360-degree process in order to guarantee that a breach of data does not occur on either an internal or external level. This is a process of protecting the customer-facing side of processes undertaken in banking and also in the internal processes involving employees, vendors and systems. The following are five ideas on how to protect data in the banking sector: authentication, audit trail, secure Infrastructure, secure Processes and so on. Authentication-wise, authentication proposes that all transactions in the bank must be made only after verifying the identity of the individual who is submitting the transaction. This would be on customers who are accessing online or mobile banking, those going to the bank physically or those who are using the credit/debit cards at the POS terminals and ATMs. It is also relevant to the bank employees who have access to the information on customers and banks. Whereas previously authentication was as easy as an ID and a password or PIN, nowadays, in order to be sure that it is not an imposter but rather a real person, two-factor authentication multi-factor authentication have been employed in many banks. Similarly, banking institutions are also employing biometric verification methods to authenticate a customer's identity, such as behavioural biometrics when accessing such

banking systems as the Interactive Voice Response (IVR). This becomes a very critical component of the general information security plan of the bank. With regard to audit trails, they had a history of banking transactions always available as a statement or passbook. There is also an audit trail according to what is being used in banking systems, where every event that happens when a customer interacts with the systems is taken care of. This is important in order to react fast to incidents such as a security breach or a ransomware attack. It is a case of both a customer who accesses phone banking and an online customer, and the time of the call is noted alongside the information of the call. Such information is backed up every day, and it is never deleted externally but rather archived at specified time intervals. Some of the audit trails involve having a security incident response plan. Both in the secure Infrastructure, Sidney et al. (2022) recommended that securing the infrastructure directs efforts towards the database systems as well as the servers on which they are stored in addition to developing boundaries that must be imposed to keep them secured. Any core banking system has a tendency to encrypt production data. Production systems are limited in access and only approved providers administer vital infrastructure. These databases can be secured by effective access management. Any critical information such as bank account number, customer name and address, is subject to masking in case it is needed for testing. Most likely, there are differences between the vendors who are dealing with infrastructure and those who are dealing with applications. Employees in banks would mostly be provided with special equipment, access to social sites, personal emails, and USB ports are denied. When working on public WiFi, employees are only allowed to use VPN in accessing the network of the banks.

On secure processes, Shamir (2017) noted that banks must put in place numerous processes that would guarantee that security is enforced and verified. As an example, the Know Your Customer (KYC) update on the part of the customers, non-disclosure agreement (NDA) on the part of the employees and vendors, and gaining access to special sections of the premises and remote data centres. Commercial banks could counter the risk of insider attack and protect the personal information, such as names and credit card numbers of the customers using data Loss Occurrence (DLP) solutions. Such solutions that Rafi (2024) advocates can also aid the need to enjoy regulatory compliance with the data protection regulations like PCI DSS and GDPR, and by so doing, ensure that the security of any banking establishment adopts the consensus standards and safeguards the information held on behalf of that bank. Global and local regulations related procedures are also executed, and risk assessments are also conducted to ascertain that these procedures are as per the requirements. Regarding consistent communication, the consumer is always in contact with the commercial banks about changes in the system and the addition of new forms of authentication. Besides the periodic account statements, which are prepared and presented to customers. The customers may also extend to establish limits and alerts relative to various terms to ensure that cases are communicated in case of any unforeseen occurrences of activities to be carried out relating to their accounts. In spite of varying channels of communication, the set-up is flexible to meet the convenience of the customers. Endpoint Protector in strengthening Data Security. These five tips make sure that personal and financial information of the commercial bank is not at risk. It is also important to deploy different security solutions to protect the data of customers.

Authentication and Prevention of Fraud Occurrence

The process of identifying someone, or something, is authentic and is known as Authentication. Karen et al (2014) note that authentication is the process through which companies verify that only the right people, services and apps have the permission with which they can access organisational resources. It plays a big role in cybersecurity since unauthorised entry to the systems by a malicious actor is his or her number one priority. Karen et al further claimed that authentication technology supports access control on systems by authenticating whether the credentials used by the user are similar to those enlisted in a database containing a list of authorised users or a data authentication server. By so doing, we should expect authentication to secure systems, processes and information in the enterprise. According to Leandros and Nick (2022), the types of authentication are several. These are user identity ID, single-factor authentication, 2 factor authentication, and authentication protocol, among others. In user identity, users are normally known by a user ID; authentication is achieved as long as the user inputs credentials, alias: a password, that is the same as their user ID.

Single-factor authentication (SFA) is the practice of the use of the user ID and password. Organisations in the past few years have enhanced authentication by requesting extra authentication parameters, as stated by Karen et al (2014). These may include something like a unique code given to a user via mobile agent when they would like to sign on or a biometric usage e.g. a scan of the face or thumb print. This is what is referred to as two-factor authentication (2FA).

Authentication protocols may be extended beyond 2FA and employ several factors to an individual or device. Such authentication models, where two or more factors are entailed as claimed by Huan et al (2020) are referred to as multifactor authentication (MFA). Human et al also believed that three main steps involve the process of authentication, and they are identification, authentication and authorisation. When it comes to identification, users determine their identity in most instances by use of a username. Regarding authentication, users usually authenticate themselves by providing a password (something only the user is expected to know), but to improve security, most organisations today insist on authenticating a user with something they have (a phone or a token device) or something they are (fingerprint or face scan). Regarding authorisation, the system determines whether the users have access to the system or not, to which they are trying to log in. They accomplish this by stealing the usernames and passwords of those individuals who can access.

Authentication is significant, according to Matuishin and Korkhova (2022), since it assists companies in securing their systems, information, network, websites, and apps against attacks. It also aids people in generalising their personal data as a way to have them in protection and enable them to do what would be considered business, e.g. banking or investing and do it online and be at less risk of doing so. In cases when authentication processes are fragile, as hypothesised by Matuishin and Korkhova (2022), an attacker can hack an account by guessing the passwords of individual users and by deceiving individuals into posting their credentials data. This may attract the following threats, as indicated by Matuishin and Korkhova: Data leakage or exfiltration. Malware application, including ransomware. Failure to comply with data privacy laws in a region or an industry. In the case of persons, Matuishin and Korkhova (2022) mentioned that the process of authentication implies the creation of a username, a password, and other means of authentication with the help of which a person can be recognised (a facial scan, fingerprint, or PIN). None of these authentication types is

stored in the databases of the service to preserve identities. The passwords are not encrypted, but hashed and then stored in the database. When the user inputs a password, the password inputted is also hashed, and the resulting outputs are compared. When the two hashes are similar, the access will be granted. In the case of Fingerprint and face scan, these printouts will be encoded, encrypted, and stored in the device.

In modern authentication, the authentication process is outsourced to an outside trusted identity system, and the usual approach is that in traditional authentication, each system authenticates itself. The type of authentication methods has also changed. Username and password are, of course, needed in most applications, but since the bad guys have become clever in hacking into passwords, the security fraternity has come up with a number of novel ways to help secure identities. As far as password-based authentication is concerned. The most widespread is password-based Authentication. Various services and applications require individuals to create passwords that rely on a mixture of numbers, letters, and characters to ensure that a malicious actor does not have a high chance of guessing them. Nevertheless, passwords are associated with usability and security problems. Human beings can hardly think of several unique passwords to remember all their web accounts, and this is why they frequently repeat passwords. Attackers have a lot of tricks to find or steal a password or to make people unwillingly share it. It is in view of this that organisations are migrating to more secure authentication methods other than passwords. Regarding certificate-based authentication, Matuishin and Korkhova (2022) described that certificate-based authentication is an encrypted mechanism that allows machines and individuals to recognise themselves to other machines and systems. Two typical instances are with a smart card or when a gadget of an employee transmits a digital certificate to a network or server. When it comes to biometric authentication, individuals identify themselves with the use of biological features. As an example, a lot of people use their fingers or thumbs to log into their phones, and some computers are going to scan the retina or face of a person for an identity check. The biometric data is also associated with a particular gadget, hence hackers cannot use them unless they get access to the gadget as well. This form of authentication is getting more popular since people find it simple, one does not have to memorise it, it is not easily stolen by bad actors, and thus safer than passwords.

In terms of simplified login and transaction processes, Huan *et al*. (2020) stated that some authentication methods, like biometrics, can streamline the login process and make transactions faster and more convenient for customers. In improved access management, Leandros and Nick (2022) asserted that authentication allows banks to control access to specific information or functionalities, providing users with the right level of access to their accounts, according to Fortinet. Business benefits are not left out. In terms of compliance with regulations, many banking regulations require specific authentication measures to protect customer data and ensure the security of financial transactions. In terms of increased efficiency, streamlined authentication processes can improve operational efficiency, reducing the workload on customer service teams and allowing them to focus on more complex issues. Enhanced reputation and brand loyalty are still part of the business benefits. By prioritising security and customer trust, banks can build a stronger reputation and foster greater customer loyalty. In terms of growth in emerging economies, biometric authentication, in particular, can be crucial in expanding banking services to populations that may lack traditional identification

documentation, as noted by International Banker. The authentication process is shown in the figure:

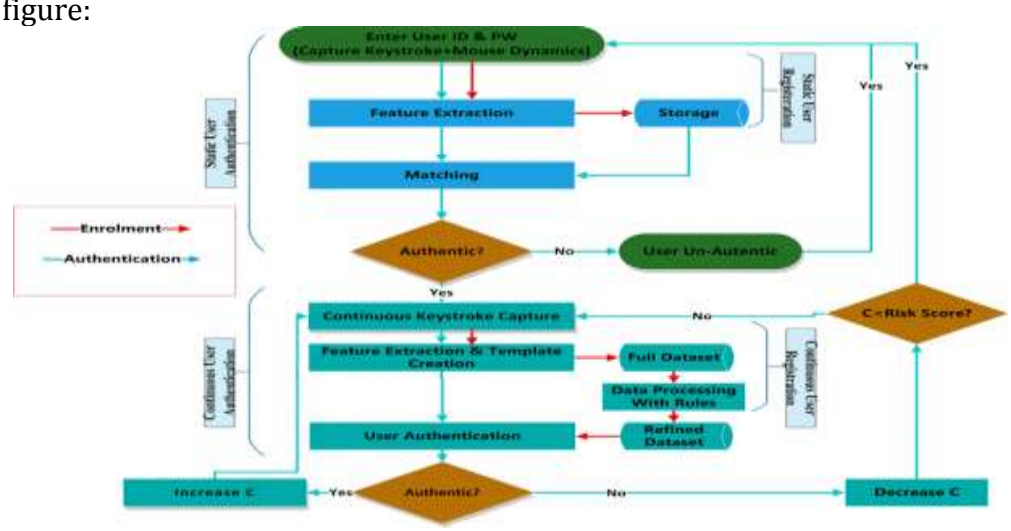

Figure 2.6: The Authentication Process

METHODOLOGY

A 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 sample consists of 32 managers, 32 accountants, and 218 cash officers. Taro Yamane's formula will be applied to choose the sample. The researcher developed a structured instrument titled: Emerging Technologies and Prevention of Fraud Occurrence (ETPFQ) for data collection. Face and content validation were used. The analysis of the data obtained was done in Cronbach's 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.

RESULTS AND DISCUSSION

Research Question One

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

Table 1: Summary of mean on extent of use of data encryption to prevent fraud occurrence in commercial banks N=282

S/N	DATA ENCRYPTION	Mean	Std. Dev.	Remark
1.	secret-key encryption	3.44	0.90	GE*
2.	Asymmetric encryption, where there are 2 keys	3.39	1.12	GE
3.	Attribute-Based Encryption (ABE)	3.16	1.06	GE
4.	Key Generation techniques	3.25	0.95	GE
5.	Key Storage/retrieval	3.52	0.69	VGE**
6.	Key Distribution	2.91	1.27	GE
7.	Implement Comprehensive Key Management	3.04	1.31	GE
8.	Rotate encryption keys to minimise the risk of key compromise	1.92	1.21	LE***

9.	Properly destroy old or obsolete keys to prevent potential misuse	3.04	1.22	GE
10.	Regular Updates and Patching	3.77	0.62	VGE
	Cluster Mean	**3.14**	**1.03**	**GE**

*GE- Great Extent; **VGE- Very Great Extent, 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 data encryption prevents fraud occurrence in commercial banks. The result shows that the mean range is 1.92-3.52. The standard deviation ranges from 0. 69 - 1.31, indicating that the responses cluster around the mean and are not too dispersed from each other. The result shows that all the items have a mean within 2.50 -3.49, indicating there is a very great extent to which the use of data encryption prevents fraud occurrence. The cluster mean of the responses is 3.14. This indicates that there is a very great extent to which the use of data encryption prevents fraud occurrence in commercial banks in South-South, Nigeria.

Research Question Two

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

Table 2: Summary of mean of extent of use of authentication to prevent fraud occurrence in commercial banks N=282

A	AUTHENTICATION	Mean	Std. Dev.	Remark
1.	Making use of passwords	3.54	0.87	*GE
2.	Having security token	3.54	0.85	**VGE
3.	Utilises biometric information	3.16	1.04	GE
4.	Making use of fingerprint	3.09	1.10	GE
5.	Having facial recognition	3.17	1.12	GE
6.	Making use of voice recognition	3.52	0.91	VGE
7.	Verifying identity	3.52	0.87	VGE
8.	Using biometric authentication	3.22	1.15	GE
9.	Using wireless networking technology	3.35	1.00	GE
10.	Having smart cards	3.56	0.92	VGE
	Cluster Mean	**3.37**	**0.98**	**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 authentication prevents fraud occurrence in commercial banks. The result shows that the mean range is 3.09-3.56. The standard deviation ranges from 0.87-1.12, indicating that the responses cluster around the mean and are not too dispersed from each other. The result shows that all the items have mean within 3.50 – 4.00 indicating that there is a very great extent to which the use of authentication prevents fraud prevention. The cluster mean of the responses is 3.37. This indicates that there is a very great extent to which the use of authentication prevents fraud occurrence in commercial banks in South-South, Nigeria.

Hypothesis Testing

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 data encryption prevents fraud occurrence in commercial banks in South-South, Nigeria.

Table 3: 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 data encryption prevents fraud occurrence in commercial banks

		Sum of Squares	Df	Mean Square	F	Sig.
Using algorithms to transform plaintext into ciphertext	Between Groups	10.542	2	5.271	6.717	.110
	Within Groups	218.933	279	.785		
	Total	229.475	281			
Securely managing access to encryption keys	Between Groups	44.697	2	22.348	20.350	.072
	Within Groups	306.395	279	1.098		
	Total	351.092	281			
Protecting data from unauthorised access	Between Groups	23.872	2	11.936	11.513	.331
	Within Groups	289.262	279	1.037		
	Total	313.135	281			
Implementing robust key management practices	Between Groups	23.281	2	11.640	14.161	.101
	Within Groups	229.343	279	.822		
	Total	252.624	281			
Implementing encryption to comply with regulations	Between Groups	3.651	2	1.826	3.898	.121
	Within Groups	130.675	279	.468		
	Total	134.326	281			
Monitoring encryption performance	Between Groups	88.629	2	44.315	34.063	.101
	Within Groups	362.973	279	1.301		
	Total	451.603	281			
Protecting sensitive data	Between Groups	111.139	2	55.570	41.845	.131
	Within Groups	370.506	279	1.328		
	Total	481.645	281			
Avoiding modifications of data	Between Groups	.715	2	.358	.245	.783
	Within Groups	407.569	279	1.461		
	Total	408.284	281			
Minimises the risk of data breaches	Between Groups	124.247	2	62.124	58.706	.101
	Within Groups	295.242	279	1.058		
	Total	419.489	281			
Improves the security of digital communication	Between Groups	2.233	2	1.117	2.905	.056
	Within Groups	107.242	279	.384		
	Total	109.475	281			
						,191

Table 3 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 blockchain to prevent 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 .191. Since p>.05 .191, 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 data encryption prevents fraud occurrence in commercial banks in South-South, Nigeria.

Hypothesis Two

There is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of authentication 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 authentication prevents fraud occurrence in commercial banks

		Sum of Squares	df	Mean Square	F	Sig.
	Between Groups	47.991	2	23.995	40.330	.151
	Within Groups	165.999	279	.595		
Making use of passwords	Total	213.989	281			
	Between Groups	46.506	2	23.253	41.703	.110
	Within Groups	155.565	279	.558		
Having security token	Total	202.071	281			
	Between Groups	128.023	2	64.011	100.836	.072
	Within Groups	177.112	279	.635		
Utilises biometric information	Total	305.135	281			
	Between Groups	117.613	2	58.806	73.791	.083
	Within Groups	222.345	279	.797		
Making use of fingerprint	Total	339.957	281			
	Between Groups	128.968	2	64.484	81.458	.113
	Within Groups	220.862	279	.792		
Having facial recognition	Total	349.830	281			
	Between Groups	.180	2	.090	.109	.897
Making use of voice	Within Groups	230.146	279	.825		
recognition	Total	230.326	281			
	Between Groups	2.445	2	1.222	1.625	.199
Making use of voice	Within Groups	209.927	279	.752		
recognition	Total	212.372	281			
	Between Groups	24.543	2	12.271	9.942	.110
	Within Groups	344.383	279	1.234		
Using biometric authentication	Total	368.926	281			
	Between Groups	53.524	2	26.762	32.688	.090
Using wireless networking	Within Groups	228.419	279	.819		
technology	Total	281.943	281			
	Between Groups	7.025	2	3.512	4.290	.715
	Within Groups	228.450	279	.819		
Having smart cards	Total	235.475	281			
						.254

Table 4 presents a 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 authentication to prevent 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 .254. Since $p > .05$, 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 authentication prevents fraud occurrence in commercial banks in South-South, Nigeria.

CONCLUSION

The study concluded that data encryption and authentication remain vital tools in safeguarding financial data and transactions in commercial banks within South-

South, Nigeria. Their proper adoption significantly reduces the risk of unauthorised access, identity theft, and fraudulent activities. Banks that invest in these technologies foster trust and confidence among customers. However, their effectiveness depends on continuous upgrading to counter evolving cyber threats. Staff training and compliance with security policies are equally critical to sustain their relevance. The study showed that there is no significant difference in the mean responses of managers, accountants and cash officers on the extent to which the use of data encryption and authentication prevents fraud occurrence in commercial banks in South-South, Nigeria.

RECOMMENDATIONS

1. Commercial banks are advised to adopt a 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 other regulations.
2. Commercial banks ought to focus on powerful authentication methods such as multi-factor authentication and sound password policies that restrict data exploitation to customers and curtail fraud.

REFERENCES

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.

Ezeofor, C. J. and Ulas, A. G. (2014). Analysis of network data encryption and description technologies in communication system. *International Journal of Innovative Research in Science, Engineering and Technology,* 1(1): 10-21.

Martin, V. (2021). *Bitcoin Network Shaken by Blockchain Fork.* Available: https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/. (Accessed 29 August 2022).

Matuishin and Korkhova (2022),

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.

Rafi, J. (2024). Data encryption and privacy in cloud banking: Best practices and regulatory compliance. *Research Journal of Modernisation in Engineering Technology and Science,* 6(4): 39-45. Doi:10:56726/iRSMETS53838.

Shamir, A. (2017). Chaotic rivesrs-shamir-Alderman Alogarithm with data encryption standard scheduling. *Bulletin of Electrical Engineering and Informatics*. 6(3): 219-227.

Sidney, K. and Mubukwanu, K. (2022). *Mitigating Cybersecurity Risks in the Digitization of Banking Operations: Strategies, Challenges and Best Practices for Zambia Commercial Banks.* IDEAS Publishers, Zambia.

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

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

Zadia, V. L. (2021). *To Blockchain or Not to Blockchain: That is the Question*. [Online]. Available: https://www.researchgate.net/publication/324551383_To_Blockchain_or_Not_to_Blockchain_That_Is_the_Question. (Accessed 27 August 2022).