

# FRAUD PREVENTION IN A DIGITAL ENVIRONMENT: ISSUES AND PROSPECT

<sup>1</sup>YESUFU, NASIRU IKIEBE (PhD), <sup>2</sup>IGBINOSUN FRIDAY ESE (PhD)

<sup>1</sup>Department of Accountancy  
Federal Polytechnic, Auchi, Edo State, Nigeria.

<sup>2</sup>Accounting Department  
Glorious Vision University Ogwa, Edo State, Nigeria.

DOI: <https://doi.org/10.5281/zenodo.16737139>

Published Date: 04-August-2025

---

**Abstract:** The study investigated fraud prevention in a digital environment: issues and prospect. Sample size of 330 derived from a total study population of 1,889 using Taro Yamane statistical formula in the study. Questionnaire was used as the instrument of data collection and the data collected were analysed using simple percentage while hypotheses was tested using t-test. From the analysis of the data and test of hypotheses, result shows that digital forensic accounting environment offers investigators more reliable and efficient avenue to uncover financial fraud. Digital forensic accounting environment help minimize the extent of financial fraud since it expose detailed information on the processes used in the financial fraud as well as exposes more detailed information to the investigator. It's in the light of this that the study therefore recommends that digital forensic investigation method should be adopted fully by forensic accountant in other to aid investigation and give more reliable and efficient information that will enable them carry out their duties perfectly.

**Keywords:** fraud instigation, forensic investigation, fraud prevention, financial fraud, digital environment.

---

## I. INTRODUCTION

### *Background to the Study*

The modern digital environment offers new opportunities for both perpetrators and investigators of fraud. In many ways, it has changed the way fraud examiners conduct investigations, the methods internal auditors use to plan and complete work and the approaches external auditors take to assess risk and perform audits. While some methods, such as online working papers, are merely computerized versions of traditional tasks, others, such as risk analysis based on neural networks are revolutionizing the field (Conan, 2024).

Many auditors and researchers find themselves working amid an ever changing workplace, with computer based methods leading the charge. Perhaps the most difficult aspect to computer based techniques is the application of a single term to a wide variety of methods like digital analysis, electronic evidence collection, data mining, and computer forensics. Indeed, computer based fraud detection involves a plethora of different technologies, methodologies and goals. Some techniques require a strong background in computer science or statistics while others require understanding of data mining techniques and query languages. In today's digital environment, digital based fraud detection techniques in most accounting circles revolve around the use of Benford's Law to discover false invoices or other fraudulent amounts in corporate databases. Analysis of data against Benford's distribution is useful, but it is only one of many computer based fraud detection techniques that is invocation in this digital age.

In many countries today, Nigeria inclusive, financial fraud has hindered adequate growth and hampered the welfare of the citizens. This has led to a lot of economic under development and poor social responsibilities toward the citizens (Okunbor & Obaretin, 2020). As time goes by, perpetrators of financial crime have advanced to more complex form of fraud system which as well makes it difficult for auditor to sometimes detect areas in financial statement that has being altered in other

to be able to successfully cover a lot of public funds among others. This has necessitated the need for more complex and advanced techniques such as the use of digital forensic methods for detecting and preventing financial frauds (Bassey, 2018). It is against this background that this study focuses on fraud prevention in a digital environment as well as some issues and prospects associated with it.

### ***Statement of the Problem***

Financial corruption and other forms of frauds have made it more difficult for Nigeria as a country to meet her welfare and social responsibilities towards its citizens. This has resulted to a great proportion of financial mismanagement of resources both in the private and public sectors (Okunbor & Obaretin, 2020). Financial fraud has indeed become a really pervasive issue in Nigeria and the likelihood of corporate financial crime to occur has become more severe as compared to what it used to be before this digital age (Okolo, 2022). Problem of financial fraud hinders effective tax collection and hinders foreign investment which has a direct or indirect negative effect on the growth of the economy as well as affect the standard of living. The wide spread of financial fraud in public sectors in this digital environmental age has made traditional auditing and investigation to become more inefficient and ineffective to detect fraud.

In Nigeria, the incessant increase of financial fraud in public sectors is creating a serious negative wave on the growth and development of the country. This has created a greater responsibility and functions on Accountants to be well equipped in this digital age to acquire the skill needed to identify traces of financial fraud in poor corporate governance, mismanagement, fraud and wrong doings. Hence, the failure of auditors to prevent, detect and reduce modern frauds like white collar crimes such as security fraud, embezzlement, bankruptcies, contract disputes, money laundering among other financial crimes in the public sector has put pressure on professional accountants and legal practitioners to find better ways of exposing fraud in public sector (Akinbowale, 2018). It is on this account that necessitated this study to focus on fraud prevention in a digital environment: issues and prospects.

### ***Objectives of the Study***

The major objective of the study is to ascertain the issues and prospects of fraud prevention in digital environment. Specific objectives are to ascertain;

1. The extent the prospect of Ensemble Modeling in fraud prevention in a digital environment.
2. The prospect of Human-in-the-loop for fraud prevention in digital environment.
3. Issues in the use of computer based fraud prevention in digital environment.
4. Issues of cloning dictation in fraud prevention in digital environment.

### ***Research Questions***

In order to achieve the objectives of the study, the following research questions are posed to guide the conduct of the study as follows

1. To what extent do prospects of Ensemble Modeling in fraud prevention in a digital environment?
2. What are the prospects of Human-in-the-loop for fraud prevention in digital environment?
3. What are some of the Issues in the use of computer based fraud prevention in digital environment?
4. What are the Issues of cloning in fraud prevention in a digital environment?

### ***Hypotheses***

The following null hypotheses are posed to test each of the research findings of the study as follows.

Ho1: There is no significant prospect of Ensemble Modeling in fraud prevention in a digital environment

Ho2: Prospect of Human-in-the-loop for fraud prevention is not significant in digital environment.

Ho3: There are no significant Issues in the use of computer based fraud prevention in digital environment.

Ho4: Issues of cloning in fraud prevention is not significant in a digital environment

## II. REVIEW OF RELATED LITERATURE

### *Conceptual Framework*

#### **Fraud**

According to financial dictionary (2012), fraud is any attempt to deceive an entity, be it individual, organization, government or the society for personal financial gain. Steven (2018) defining fraud from accounting view point said that fraud is it is intentional manipulation of financial statements to create a facade of a company's financial health. According to him, it involves an employee, account or the organization misleading investors and shareholders by falsifying its financial statements by overstating its revenue or assets, not recording expenses and under-recording liabilities. While CBN (2010) defined fraud from financial point of view to intentional act of deception involving financial transactions for purpose of personal gain.

#### *Forensic accounting*

James (2018) defined forensic accounting as the aspect of accounting that utilizes accounting, auditing and investigative skills to conduct an examination into the finances of an individual or business. While forensic digital environment according to Global (2019) is a context, or a place, that is enabled by technology and digital devices, often transmitted over the Internet, or other digital means such as computer among others.

#### *Forensic digital environment*

Hensel and harper (2016) also defined a forensic digital environment as an integrated communications environment where electronic, or digital devices are the tools which communicate and manage the content and activities. Therefore, from the above, a forensic digital environment can be said to be the use of digital technology and tools in the detection of fraud in any given financial environment.

#### **Theoretical Framework**

The study is anchored on theory of white collar crime and technological theory

**White collar Crime Theory:** This theory of white collar crime was propounded by Sutherland in 1949. State that white-collar criminals are opportunists either in public or private sectors who over time learn to take advantage of their circumstances or position to accumulated financial gain and as well advances in their technique of financial fraud day by day. According to this theory, the white collar criminal are educated, intelligent, affluent, individuals who are qualified enough to get a job which allows them the unmonitored access to often large sum of money to enrich themselves in detriment of others. The use of those theory in those study is appropriate since it will expose new ways of fraudulent attitude in order to prevent it.

**Technological Theory:** This theory was propounded by Marshal McLuhan in 1999. The theory state that technological advancement is influenced by the behavior of human within a given society with their various cultures. This theory assumes that as human behavior changes from day to day, so also there will be more advancement in technology to suit the current change of human behavior. These theories suite the study since the study is aimed at fraud prevention in digital environment. The theory is also appropriate since financial perpetrators advances in their criminal techniques day by day hence, the need in advancement in ways in exposing financial fraud using a more advanced digital medium.

#### *Theoretical Exposition*

The review of related literature is discussed under the following subheading;

#### ***The Prospect of Ensemble Modelling in fraud prevention in a digital environment.***

fraudsters are always in the lookout to find new and innovative ways in this digital age to get around the systems to commit the fraudulent act. Thus it becomes all-important for the deep learning models to be updated with the evolved patterns to detect fraudulent activities. This results in a decrease in the model's performance and efficiency. Thus the machine learning models need to keep updating which bring about that ensemble modelling in this modern digital age. To tackle the ever-evolving fraudulent patterns, Ensemble modeling leverages multiple models for a single task such as fraud detection. Ensembling with classic machine learning, deep learning, and linear models can capture various fraud patterns to maximize

outputs. For example, an LSTM (Long Short Term Memory) deep learning model is useful for detecting fraud in a sequence of events. If a user logs in with a new IP address from a different city, changes his street address on file, then purchases an expensive item on an e-commerce site, LSTM might flag this transaction as fraudulent (Razorthink, 2019). None of these events alone is indicative of fraud, but the sequence of all three is.

According to Center for financial reporting reform (2016), classified fraud into public and private sector fraud.

**Public sector fraud:** In public sector fraud, issues such as bribery, corruption, and misuse of authority during public procurement often come to mind. These practices usually involve misuse of entrusted power for personal gain, often including cash given under the table so there is very little or no financial statement evidence that a crime has occurred. Such crimes are uncovered in most cases through tips or complaints from third parties, often via a fraud hotline or are detected during internal reviews, external audits, and by financial inspections (Vias, 2019).

Frauds within the public sector, including State-Owned Enterprises (SOEs), originate from both internal and external sources. Internal frauds can be committed by any employee at any level within the organization. They can range from small-scale abuse of travel expenses to large-scale frauds involving high-value contracts and breaches of controls that could have serious and material consequences. Other examples of fraud and illegal activities include money laundering (the transforming of profits of crime and corruption into legitimate assets); tax evasion (the deliberate reporting of false information in tax reporting); and informality (economic activity that is not taxed or monitored by governments).

**Private Sector Fraud:** This type of fraud and includes bribery, political corruption, business and employee fraud, consumer theft, network hacking, bankruptcy and divorce fraud, and identity theft. Business fraud often called occupational fraud also all among this category of fraud and often is usually most interesting to accounting professionals (ACFE, 2018). It also includes schemes like employee embezzlement and kickback relationships. Internal fraud is usually found by internal auditors or dedicated fraud detection teams through hotlines, data mining efforts, and internal audit (Albrecht, *et. al.*, 2018). Other forms of this type of fraud involve external business fraud, or financial statement fraud, involves schemes on behalf of a company. This is most often done by misrepresentation of the financial statements to improve company image and mislead stockholders and other interested parties (Ogbeide, 2018). The external schemes in this category involve revenue and inventory overstatements, liability understatements, inadequate disclosure fraud, and other manipulations to the financial statements and company records (Wells, 2012).

The act of fraud investigation is comprised of several activities, including initial discovery, public record search, interviews of various types, document recovery and search, legal prosecution, and computer forensics. The typical fraud investigator is heavily involved with many of these activities, but he or she generally works with legal counsel or information security professionals for more specialized tasks. Even within the relatively narrow field of computer based fraud detection, significant differences in task performance and knowledge requirements exist. For example, computer forensics requires knowledge of disk cloning, operating systems, file and graphics formats, and scripting for automation. In contrast, data theft prevention and investigation requires knowledge of databases, security, intrusion detection, hacking principles, and encryption (Wells, 2012).

#### ***The prospect of Human-in-the-loop for fraud prevention in digital environment.***

This technique addresses the classification imbalance issue as well as shortens the time taken for feature fraud detection. It involves humans assisting the models by providing information to identify new patterns of fraud features, and dimensions of fraud. In the preceding e-commerce use case, for instance, a human could denote that such a sequence was indicative of fraud. The model will then extrapolate this information and apply it to different use cases, such as when users change email addresses instead of physical addresses. Based on human input, the model learns from these examples then identifies more from its own learning (Razorthink,2019). Several digital forensic accounting tools are available and used in the detection of fraud. According to Sulaiman *et al.*,(2015) the various tools that are used In digital forensic accounting environment include, digital investigation manager(DIM), Encase, Computer Aided Audit Tools (CAAT), Forensic Toolkit (FTK), Helix, Incident Response tools for Operating Systems, Browse contents of the CD-ROM and Host OS, ACL Desktop, UltraBlock, Advance Hash Calculator and Passware Kit Forensic.

**a) Digital Investigation Manager (D.I.M):** This is a digital evidence tracker software used in digital investigations. It was designed and developed to be used as digital evidence process support during computer forensic and incident response

operations (ACOU,2011). It allows the investigation process to be organized on a case basis as each case may contain one or more hosts (i.e. workstation, laptop, etc.), which in turn may be associated with one or more items of evidence obtained through the forensic acquisition process. This forensic acquisition process include media (hard disk, floppy disk, flash card zip driveetc.), network dump and log file. Special detailed forms are usually compiled for each of these host or media when they are acquired. Also, the digital investigative manager application allows users to catalogue all pertinent information gathered during investigation and to make reports from those evidence gathered. This application is usually available in three (3) versions namely, standalone version, workgroup version and enterprise version (Forensic Focus, 2023).

Digital Investigation Manager also offers a variety of data security and team coordination options. It allows the user to create a copy of local data in a centralized archive. This has a dual purpose: the user is assured of having a copy of the work performed and a central historical record is maintained for all cases involving a particular investigator. The backup option requires a properly configured back-end database server. Supervisors may access the back end for itemized queries (Forensic Focus 2023).

**b) Encase:** This is a complete forensic toolkit that covers much of the work that the ITM (information technology management) forensic analysis carry out. It is designed as “a computer forensic product produced by guidance software used to analyses digital media in civil or criminal investigations, network investigations, data compliance and electronic discovery”. Encase contains tools for several areas of the digital forensic process, acquisition, analysis and reporting.it is usually available to law enforcement agencies and corporations, for it has been used successfully in various court systems around the world. It is also generally considered as the de factor standard for criminal digital forensic evidence collection as it is globally recognized as a world leader in digital forensic, cyber security and e-discovery (Oliver & Sheno, 2020).

The two (2) major attributes that make Encase software unique are the breadth of operating system and file system are separate, but they have a deep relationship on how information is stored and how the host operating system operates system that exists, there are number of different file system which the host operating system could utilize and the ability to deeply analyses a broad range of operating system and file system is a critical component of an enterprise investigation. (Guidance, 2014).

Digital investigators need a solution that easily captures relevant data to support an investigation or compliance requirement and features sophisticated technical analysis capabilities for finding buried and/or hidden data. EnCase Forensic is a powerful investigation platform that collects digital data, performs analysis, reports on findings and preserves them in a court validated, forensically sound format (Guidance, 2014).

**c) Computer Aided Audit Tools (CAAT):** It is also known as Computer Assisted Audit Tools and Techniques (CAATTs), it is a growing field within the financial audit professions practice that use computer to automate or simplified the process by extracting data, analyzing data and identifying exceptions that relate to fund. Computer Aided Audit tools have a significant advantage over manual data testing techniques and they include; ACL Audit, Command language, IDEA Analysis, Wiz Rule etc. With these tools, forensic accountant can review, test and analyze the entire population of data which is not usually possible with the manual or traditional audit techniques (ACFE, 2019).

Data Mining Software is another tool that provides models of database for the purpose of determining patterns and relationships among the data. This tool is an outgrowth of the development of expert systems. Computer-based data analysis tools can prove to be invaluable in searching for possible fraud. From the analysis of data, the fraud examiner can develop fraud profiles from the patterns existing within the database. Through identifying and understanding these patterns, the examiner may uncover fraudulent activity. The use of this software also provides the opportunity to set up automatic red flags that will reveal discrepancies in data that should be uniform (Ekeigwe, 2010). Also, it tends to enhance the productivity of forensic accountant, as it enable them make informed discussion to qualify the impact of financial statement errors by analyzing them through CAAT, for CAAT gives a high level of comfort to the senior management about the overall quality of data within the organization (Just answer, 2011).

**d) The access data forensic toolkit (FTK):** This is a component forensic toolkit that is recognized as one of the leading forensic tools to perform e-mail analysis, as it can easily locate deleted e-mails. It includes a standalone disk imaging program called FTK imager. This FTK imager is a simple but concise tool that saves an image of a hard disk in one file or in segments which may later be reconstructed (Access data 2011). Also known as FTK, this application enables forensic

accountant to perform complete and thorough computer forensic examinations. FTK features powerful filtering and search functionality and is recognized by law enforcement and corporate security professionals as the leading forensic tool for e-mail analysis (Access data, 2011).

Forensic toolkit advances investigation by giving more time, power, and insight to each case. It provides the following advantages: simple users' interface, fast searching, EFS decryption, bookmarking, reporting and password dictionary creation. After completing case investigation, it create a report that summarizes the relevant evidence of the case. This digital forensic application provides a thorough report wizard that allows customization of reports, including the placement of one's own logo on the title page. The final report is in HTML format and is viewable in a standard Web browser.

It can add files such as supplementary reports, search warrant information, and photos of the crime scene to the report. It has a case log documents activities and events that occur in the case during investigation and analysis.

### ***Issues in the use of computer based and cloning fraud prevention in digital environment.***

Many organizations understand that preventing computer fraud is an important technology initiative and have instituted programs to recognize and prevent fraudulent activity. However, when preventive measures fail and computer fraud does occur, very few organizations have a plan to address and respond to the fraud attempt. The issue of preventing and responding to computer fraud is among the top ten technology initiatives, according to the AICPA's 2013 North America Top Technology Initiatives Survey, which ranks preventing and responding to computer fraud at number six out of ten for U.S. organizations and at number nine out of ten for Canadian organizations. It's no secret that the increase in information technology in this digital age has facilitated the perpetration of fraud in organizations. Companies who are most vulnerable include those who do not know how to identify IT-related fraud, do not have policies to prevent such fraud and do not have policies to prevent management override opportunities within financial related systems. If fraud does occur, these organizations may not have an appropriate plan in place to respond. Unfortunately, the "intangible" value associated with data can be significant. When data is stolen, its value is directly impacted and must be written down on the balance sheet – either when an event occurs or during the annual impairment analysis.

Phishing attacks are one are also another issues of the most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive information, hackers are using email, social media, phone calls, and any form of communication they can to steal valuable data. Businesses, and finance, are a particularly worthwhile target.

To help businesses better understand how they can work to avoid falling victim to phishing attacks, there is a need to follow the needed I.T steps to prevent such act.

### ***Empirical Review***

Osho (2017) investigated forensic accounting of Nigerian university financial systems and utilized the ex-post facto research design with descriptive and inferential statistics. Using financial and accounting data from 2005 to 2014 the study revealed that efficient financial management requires forensic accounting to oversee the processes and ensure transparency in all reports. Furthermore, through skilled forensic accountants working with relevant technology, a firm would not only enhance the efficiency in financial management and reporting but also prevent misconducts

Bhasin (2016) investigate the perspectives and prospects of forensic accounting including its contributions to the future of organizations. Of the diverse functions of forensic accountants, Bhasin (2016), revealed that the forensic reports and recommendations forwarded to the litigation team have essential roles. In this regard, the findings and reports of forensic accounting often reveal the loopholes or approaches to committing accounting frauds and the culpable parties .In addition to the legal directives to implement the recommendations of forensic accounting, organizations have the initiative to learn from the findings and improve financial management and reporting.

Kizil and Kaşbaşı (2023) investigated investment decisions made using inaccurate financial statements discourages shareholders and market trust. The due researched to investigate the various accounting scandals and eye catching frauds, with the objective of exploring the role of auditing and forensic accounting. The study was inspired by the fact that accounting scandals and frauds still occur in the 21st century when auditing is massively performed to ensure transparency, reliability, and compliance with the generally accepted accounting principles. In different jurisdictions, public oversight

bodies, independent auditing firms, and internal auditors are established and empowered to enhance the supervision of financial management and reporting processes. The study revealed that forensic accounting incorporates the functions of auditors, accountants, and internal control to detect frauds, corruption, misreporting, and malpractices in the private sector. Similarly, transparency and efficiency achieved in the accounting processes result in improved reliability in internal controls and positive public image of the organizations; these contribute to increased investments and financial performance.

Emmanuel *et al.* (2018) investigated the relationship between forensic accounting and integrity in financial statements through surveying professional accounting bodies in Nigeria. The group gathered data from 321 participants and multiple regressions applied to test the hypotheses. The study revealed that nearly 23% of the integrity of financial statements (IFS) is attributed to forensic accounting techniques. Similarly, the inclusion of forensic accounting techniques in the financial management and reporting systems improves the efficiency in the internal control functions, which translate to the overall organizational productivity, cost reduction, and profitability. Through creating or integrating forensic accountants, the business enhances the oversight and integrity employed in managing the financial statements.

Dada (2014), utilized a survey design to gather reliable empirical data for testing the hypothesis that forensic accounting could lower corruption, bribery, and embezzlement cases. Through regression analysis, he revealed that primary forensic accounting functions including fraud detection and prevention, have a significant impact in reducing corruption. Based on the findings, organizations should establish forensic accounting departments to oversee all the internal control practices and prevent fraud, bribe, or embezzlement instigated by external or internal stakeholders. Furthermore, operation in a corruption/bribe-free environment promotes the business relationships and stakeholders' confidence, which in turn, builds brand reputation, market share, and financial performance.

Salleh and Ab Aziz (2014) performed an empirical study to explore the perceptions of users on the traits, skills, and ethical values of forensic accountants, and how they influence organizational performance and profitability. While performing the forensic accounting functions including investigation, auditing, evidence gathering, reporting, and litigation, specific skills are necessary to ensure precision, accuracy, problem solving, attention to detail, and objectivity. His finding shows that the interaction between these core skills may influence the quality of forensic accounting and the associated financial benefits to the firm.

### **III. METHODOLOGY**

#### ***Research Design***

Survey research design was used for this study. This research design is one in which a group of people or items are studied by collecting and analyzing data from only a few people or items considered to be representative of the entire group (Nworgu, 2015).

#### ***Area of the Study***

The area of this study is Benin, Edo state. Benin is the state capital of Edo state and houses a lot of financial institution as well as the state Ministry of finances, Ministry of Budget and planning, ministry of industry and other government parastatals.

#### ***Nature and Source of Data***

Primary data were sourced from the respondents and used in the study. The primary data were all source from respondents in ministry of finance, ministry of budget, Ministry of commerce and industries and planning, banking institutions (Zenith Bank, Access Bank, First Bank and Gtb Bank).

#### ***Population of the Study***

The total population 1,889 was used in the study. This population was source from ministry of finance, ministry of budget, Ministry of commerce and industries and planning, banking institutions (Zenith Bank, Access Bank, First Bank and Gtb Bank). The population comprises of managers, accountant, Head of departments, internal auditors, secretaries and other staff. The table below shows the population breakdown of the study as follows;

S/N	Institution	Population
1	Ministry of finance	52
2	Ministry of budget and planning	530
3	Ministry of commerce and industries	241
3	Zenith Bank	269
4	Access Bank	285
5	First Bank	249
6	Gtb Bank	263
	Total	1,889

Source: Field Survey 2025

#### *Determination of sample Size*

The study sample size was determined using Taro Yamane sample size derivation formula shown below.

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

Where,

n= sample size

N= population of study

e= error (0.05)

#### *Samples Seize and Sample Technique*

A sample size of 330 was used in the study. The questionnaire was distributed to respondent using a purposive sampling technique that targeted a particular group of persons. The sample size used was derived from taro Yamane formula as follows;

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

$$\frac{1,889}{1+ 1889(0.05)^2}$$

$$n = 330$$

#### *Method of Data collection*

A structured questionnaire captioned “fraud prevention in digital environment, issues and prospect.” was developed by the researchers as instrument for data collection. The questionnaire items reflected the research questions used in the study. The questionnaire was divided into two sections A and B. Section: section sought personal information about the respondent. Section B is made up of four questions addressing the research questions posed.

#### *Method of Data Analysis*

Simple percentage was used to analysis the data and to answer the research question while one sample t-test was used to test the hypotheses

#### *Decision Rule*

Null hypotheses will be accepted when  $P > 0.05\%$  probability level. But when  $P < 0.05\%$  probability level, null hypothesis will be rejected.

#### *Presentation and Analysis of Data*

Out of the 330 copies of the questionnaires distributed, 25 copies were not correctly filled while 5 copies were not returned. Therefore, the researcher was left with 300 copies of the correct questionnaire that was used.

*Data Presentation*

**Analysis of key Demographic Variables**

**Table 1: Demographic Characteristics of the Study Population (N =300)**

VARIABLES	FREQUENCY	PERCENTAGE
<b>Gender</b>	165	55%
Male		
Female	135	45%
<b>Age Bracket</b>		
20-25yrs	60	20%
26-30yrs	80	27%
31-35yrs	100	33%
36-40yrs	35	12%
40 yrs & above	25	8%
<b>Marital Status</b>		
Single	160	53%
Married	101	34%
Divorced	39	13%
<b>Religious affiliation</b>		
Christian	245	82%
Muslim	55	18%

**Source: Field survey 2025**

Table 1 shows the demographic information of the respondents, from the table, 165(55%) of the respondents are male while 135(45%) are female respondents. This means that the study sought opinion from male and female gender in respect of the topic investigates. With regard to age the table indicated that 60(20%) of the respondents are in age bracket of 20-25yrs of age, 80(27%) are in age limit of 26-30yrs of age, 100(33%) are in age range of 31-35yrs, 35(12%) are in age group of 36-40yrs of age while 25(8%) are in age category of 40yrs. In respect of marital status of the respondent, 160(53%) are single, 101(34%) are married while 39(13%) are divorced. This implies that the study sought opinion from respondents of different marital status. The table also showed that 245(82%) are Christian and 55(18%) are of Muslim faith. Hence, it means that the study gathered information from respondents of different religious background with different view on environmental sanitation.

**Analysis of Research Questions**

**1. Research Question One: what are the prospect of Ensemble Modeling in fraud prevention in a digital environment?**

? Responses to the above question is shown in table 2

**Table 2: Responses to Research Question 1 (N=300)**

RESPONSES	FREQUENCY	PERCENTAGE (%)
Prevent Illegal money laundering	71	24
Liability understatements	67	22
Prevent Inventory overstatements	50	17
Financial statement fraud prevention	21	7
Embezzlement prevention	91	30
Total	300	100

**Source: Field survey 2025**

Table 2 shows that 71(24%) of the respondent are aware that Ensemble Modeling prevent illegal money laundering, 67(22%) mentioned prevention of liability understatement as another type, 50(17%) said inventory overstatements prevention, 21(7%) said financial statement fraud prevention while 91(30%) responded that embezzlement prevention is another type of financial fraud. From the responses of the respondents it implies that illegal money laundering, embezzlement, financial statement fraud among others are types of fraud that can be investigated with using digital forensic tool in digital environment.

**Research Question 2: What are the prospect of Human-in-the-loop for fraud prevention in digital environment.?**

Responses to the above Question is shown in table 3

**Table 3: Responses to Research Question 2 (N=300)**

RESPONSES	FREQUENCY	PERCENTAGE (%)
Enable Digital Investigation Manager (D.I.M)	69	23
Enables Encase	33	11
Enhance Computer Aided Audit Tools	75	25
Enhance access data forensic toolkit (FTK):	23	7
UltraBlock	12	4
ACL Desktop	45	15
Enhances Incident Response tools for Operating Systems	14	5
Strengthen Passware Kit Forensic	14	5
Enhance Prevent Advance Hash Calculator	15	5
Total	300	100

Source: Field survey 2025

Table 3 depict that 69(23%) of the respondent responded that the prospect of digital investigation manager is one of the forensic tool that enhance fraud investigation, 33(11%) Enables Encase, 75(25%) mentioned Enhance Computer Aided Audit Tools tool, 23(7%) said access data forensic toolkit is another tool, 12(4%) said ultrablock, 45(15%) mention ACL desktop, 14(5%) said that it enhances incident responses tolls for operating system, 14(5%) mentioned that it enhances passware kit forensic tool while 15(5%) mentioned that it enhance Prevent Advance Hash Calculator too. From the responses above, it implies that respondents are aware of digital forensic tool area in one way or the other making use of on the tools in fraud investigation. The results also shows that respondent are aware of the use of Human-in-the-loop for fraud prevention in digital environment.

**Research Question 3: What are the issues in the use of computer based fraud prevention in digital environment?**

Responses to the above Question is shown in table 4

**Table 4: Responses to Research Question 3 (N=300)**

RESPONSES	FREQUENCY	PERCENTAGE (%)
Lack of adequate I.T training skill	136	45
Inability use computer applications and software to trace fraud	121	41
Inability to detect and flag off fraud cases	33	11
No adequate facilities to curb fraud	10	3
Total	300	100

Source: Field survey 2025

Table 4 shows that 136(45%) agree that lack of adequate I.T training skill is one of the issues in computer based fraud control 121(41%) agree that Inability to use computer applications and software to trace fraud is another issue 33(11%) said Inability to detect and flag off fraud cases while 10 (3%) said No adequate facilities to curb fraud in digital environment is another issue. The high response of the respondents indicates that even in the digital environments, there arise issues that affect the use of digital devices in the control of fraud.

**Research Question 4: What are the issues of cloning dictation in fraud prevention in digital environment?** Responses to the Above Question is shown in table 5

**Table 5: Responses to Research Question 4 (N=300)**

RESPONSES	FREQUENCY	PERCENTAGE (%)
Failure problem	171	57
Difficult to use	89	30
Not really accurate	32	11
Can be manipulated	8	2
Total	300	100

**Source: Field survey 2025**

Table 5 shows that 171(57%) of the respondents agree that the use of digital forensic a counting has issues of failure problem, 89(30%) said it's difficult to use, 32(11%) said its not really accurate while 8(2%) responded that it Can be manipulated. From the responses of the respondent is can be seen that the use of cloning to trace fraud is has issues and cannot be 100% reliable when used alone.

**Test of Hypotheses**

**Hypothesis 1:** There is no significant fraud management type in digital environment.

in digital environment.

**Table 6: One sample t-test computation on types of fraud**

Variable	N	Df	t-value	Sig
Financial fraud	5	4	4.087	0.003

P<0.05%

Table 6 shows that all the types of fraud are significant. Since P<0.05% (Sig at 0.02) null hypothesis is rejected. Therefore, the types of fraud listed above are all significant in digital environment.

**Hypothesis 2:** There is no significant tool used in fraud management in digital environment.

**Table 7: One sample t-test computation on tools used in digital forensic accounting Environment**

Variables	N	df	t-value	Sig
Digital forensic tools	9	8	4.087	0.002

P<0.05%

Table 7 shows P<0.05% (Sig at 0.02) hence null hypothesis is rejected. Therefore, digital forensic tools are significant in forensic accounting environment.

**Hypothesis 3:** There is no significant efficient computer based fraud management in digital environment.

**Table 8: One sample t-test computation on efficiency of computer based forensic accounting in digital environment.**

Variable	N	Df	t-value	Sig
Efficient of computer forensic	4	3	2.389	0.048

P<0.05%

Table 8 shows P<0.05% (Sig at 0.048), at this level of significance null hypothesis is rejected. Therefore, computer base forensic accounting is efficient

**Hypothesis 4:** There is no significant extent to which fraud management contribute to checkmate financial fraud in digital environment..

**Table 9: One sample t-test Computation on Extent Digital Forensic Accounting checkmate Financial Fraud**

Variables	N	Df	t-value	Sig
Extent Digital Forensic Accounting checkmate Financial Fraud	4	3	2.070	0.040

P<0.05%

Table 9 shows P<0.05% (Sig at 0.048), at this level of significance null hypothesis is also rejected. Hence, digital forensic accounting help highly checkmate fraud.

#### IV. DISCUSSION OF FINDING

The findings of the study shows that there are different types of financial fraud that occurs both in private and public sectors but there are good prospect in the use of digital devices in this modern digital environment.. Some of these fraud that can be prevented with the prospect of this digital tools ranges from embezzlement of public fund, manipulation in financial statement and money laundry among others. This finding agrees with the finding of Center for financial reporting reform (2016), that reported that fraud is categorized into private and public fraud and includes embezzlement of public funds as well as money laundry. Findings also noted that digital forensic tool can be efficiently used to investigate fraud as this give better and reliable information about fraud activities. It was observed too that in digital forensic accounting there are issues in the use of digital tool some of these include lack of I.T Adequate I.T skills problems of tracing cloned data among others. This findings corroborate with the findings of Sulaiman *et al.*, (2015) who noted in that study and said that digital forensic accounting environment provide more better preventing fraud, more efficient and reliable than traditional method but has it own issues with comes as its challenge.

#### V. SUMMARY, CONCLUSION AND RECOMMENDATION

##### **SUMMARY**

From the study, it is evident that in this digital age, the use of forensic digital accounting procedure to investigate fraud is better and more efficient in this our digital age since fraud keeps advancing in our modern day society.

##### **CONCLUSION**

Evidence shows that a lot of digital tool are now available for use in forensic investigations which gives more insight to financial crime. It was also noted that when compared to traditional method of fraud investigation, digital forensic investigation have hedge since it more user friendly, efficient, not easily manipulated and gives better insight to the nature of fraud and the process used to commit it. Evidence also shows that the types of frauds can be prevented with the prospect of the digital are embezzlement of public fund, manipulation in financial statement together with money laundry, It was also conclude that the issues of using digital tool are lack of I.T adequate, I.T skill , problem of tracing cloned data. It was noted that digital forensic environment is in better position in preventing fraud not just preventing fraud but more efficient and reliable than any other methods of preventing fraud. It was also concluded that financial statement fraud are type of fraud that can be investigated using digital forensic tool in digital environment.

##### **RECOMMENDATION**

Therefore, from the result and findings from the study, the researcher recommend that digital forensic investigation method should be adopted fully by forensic accountant in other to aid investigation and give more reliable and efficient information that will enable them carry out their duties perfectly.

#### REFERENCES

- [1] Akinbowale, O. E. (2018). Information communication technology and forensic accounting in Nigeria. *International journal of Business and Financial Management Research* Vol.6(1),1-7.
- [2] Albrecht, C,Huber W, Cris,U (2018). Forensic accounting, fraud theory, and the end of the fraud triangle. *J. Theoretical Account. Res.* 12(2).
- [3] Basse, E. B. (2018). Effectof forensic accounting on the management of fraud in microfinance institutions in Cross River State. *Journal of Economics and finance*,9(4),79-86.

- [5] Conan, R(2024).Financial reporting fraud and other forms of misconduct: a multidisciplinary review of the literature. *Rev. Account. Stud.* 23(2): 732-783.
- [6] Dada S.O (2014). Forensic Accounting Technique: A means of successful eradication of corruption through fraud prevention, bribery prevention and embezzlement prevention in Nigeria. *Kuwait chapter of Arabian J. Bus. Manage. Rev.* 33(2579): 1-11.
- [7] Hensel,A.S & harper,C.E(2016) The impact of forensic auditors in corporate governance. *Res. J. Fin. Account.* 5(8):31-39.
- [8] James,A.O (2018) Forensic accounting and corporate crime mitigation. *Eur. Sci. J. ESJ.* 11(7).
- [9] Kizil C, & Kaşbaşı B (2023). Accounting Scandals and Eye-Catching Frauds: USA-Japan Comparison by Considering the Role of Auditing. *J. Asian Res.* 2(3).
- [10] Ogbeide, S. O. (2018). Empirical assessment of frauds on the financial performance of banking sector in Nigerial. *International Journal of Research Studies in Management*, 7(1), 75-84.
- [11] Okolo,J.D( 2022). Corporate sustainability reporting and stakeholder concerns: Is there a disconnect? *Accounting Horizons*, 31(1): 83-102.
- [12] Okunbor, M & Obaretin,C(2020). Forensic Accounting in Asia: Perspectives and Prospects. *Int. J. Manage. Soc. Sci. Res.* 5(7): 25-38.
- [13] Osho, T (2017) Global Economic Crime Survey 2016. Adjusting the Lens on Economic Crime.In *PwC*.
- [14] Salleh K, & Aziz R (2014). Traits, skills and ethical values of public sector forensic accountants: an empirical investigation. *Procedia-Soc. Behavioral Sci.* 145: 361-370.
- [15] Steven,O.G(2018) Forensic accounting techniques and integrity of financial statements: an investigative approach. *J. Afr. Interdisciplinary Stud. (JAIS)*: 2, 3.
- [16] Vias, A. (2019). End-User Computing Satisfaction (EUCS) toward Computerized Accounting System (CAS) in public sector. A validation of instrument. *Journal of internet banking and commerce. Vol. 16 No.2, page 2-17. Theoretical Account. Res.* 12(2).
- [17] Wells, A.E (2012). Impact of Forensic Accounting on University Financial System in Nigeria. *Eur. Sci. J.* 13(31).