SECURING FINTECH AND DIGITAL PAYMENTS: IDENTIFYING THREATS, MITIGATING VULNERABILITIES, AND STRENGTHENING DEFENSES

H. Faotu [1,*]
Esite T. J. [2]
B. T. Ebikeme [3]

Received: 18/03/2025
Revised: 13/04/2025
Accepted: 14/04/2025

[1] Department of Computer Science, Federal University of Petroleum Resources, Effurun
[2] Department of Electrical and Electronic Engineering, Nigeria Maritime University, Delta State
[3] Department of Electrical/Electronic Engineering Technology, International Institute of Tourism and Hospitality, Yenagoa
*Corresponding Author's Email: faotuhappy@gmail.com

Securing FinTech and Digital Payments: Identifying Threats, Mitigating Vulnerabilities, and Strengthening Defenses

H. Faotu
Department of Computer Science, Federal University of Petroleum Resources
Effurun
faotuhappy@gmail.com

Esite T. J.
Department of Electrical and Electronic Engineering, Nigeria Maritime University
Delta State
esite.jeremiah@nmu.edu.ng

B. T. Ebikeme
Department of Electrical/Electronic Engineering Technology, International Institute of Tourism and Hospitality
Yenagoa
benjamin.ebikeme@iithyenagoa.edu.ng

Abstract— Financial technology (FinTech) encompasses a broad range of digital solutions designed to enhance financial services through automation and accessibility. By integrating technology into banking, lending, insurance, and investments, FinTech companies streamline transactions and improve user experiences. In addition to traditional banking services, FinTech provides corporate solutions such as digital payment gateways, point-of-sale (POS) systems, and automated accounting tools. However, the rapid expansion of digital payments has also introduced significant security challenges, including identity theft, fraud, and regulatory compliance. Cybercriminals exploit vulnerabilities in online transactions, leading to financial losses and reputational damage. This study explores security risks in FinTech and the role of advanced technologies in mitigating these threats. Artificial Intelligence (AI) and Machine Learning (ML) enhance fraud detection by analyzing transaction patterns and automating real-time threat responses. Quantum cryptography and the Zero-Trust Security Model offer additional layers of security, ensuring data integrity and preventing unauthorized access. A four-layer security assessment model comprising data collection, preprocessing, presentation, and result analysis was developed to evaluate security measures. Survey findings indicate significant demographic insights into FinTech adoption. Strengthening security protocols and adhering to regulatory standards are essential for ensuring secure financial transactions and fostering trust in digital payments.

Keywords— Fintech, Security, Vulnerability, Artificial Intelligence, Technology, Digital Payment, Threat.

I. Introduction

The term financial technology, popularly known as FinTech, is a wide range of software, mobile apps, and other digital solutions intended to improve, simplify, and automate financial services for both individuals and enterprises [1]. By incorporating technology into services that banks, payment companies, and other financial organizations have historically provided, it includes a broad range of innovations that revolutionize the financial sector. FinTech solutions make banking, lending, insurance, and investing more accessible, facilitate more effective transactions, and improve customer experiences. FinTech companies offer corporate solutions in addition to traditional banking, such as digital payment gateways, point-of-sale (POS) systems, and business banking [2]. FinTech also offers automation and increased efficiency in fields like accounting, taxation, and inventory management that were previously unrelated to financial services. Also, tech firms that create payment processing, APIs, and interfaces. FinTech also offers automation and increased efficiency in fields like accounting, taxation, and inventory management that were previously unrelated to financial services. Also, the FinTech ecosystem includes tech firms that create payment processing solutions, APIs, and interfaces to improve the operations of the financial sector without having direct contact with end users. Financial institutions are always faced with security challenges, and to bridge this gap there is a need for strong security protocols to aid in shielding people and companies from online dangers, including identity theft, phishing, and hacking. Secure authentication techniques and encryption protect private financial information against breaches and unwanted access [3]. Users' confidence is increased by secure transactions, which motivates them to adopt digital payments and online banking. To protect customer data and stay out of trouble, financial institutions must abide by security regulations and standards (such as PCI DSS and GDPR). Security measures guarantee accuracy and dependability by preventing unauthorized changes to financial documents. By reducing the likelihood of fraud, chargebacks, and operational interruptions, a secure system safeguards both businesses and customers. Secure systems guarantee seamless and effective financial operations by preventing delays brought on by problems with fraud detection.

II. Background And Literature Review

A. Threat to FinTech and Digital Payment

Fintech and digital payments have revolutionized financial transactions, yet they face numerous threats. Because hackers target payment systems, there is a significant risk of cybersecurity breaches and financial theft. Another concern is regulatory obstacles, as governments impose strict compliance standards that could impede innovation [4]. Identity theft and fraud are on the rise, and criminals are taking advantage of lax authentication procedures.

Technological flaws, including software defects and infrastructure breakdowns that can halt transactions, pose a hazard as well. Smaller FinTech startups may be stifled by market competition and monopolization by larger companies, which would reduce industry variety. Furthermore, consumers who lack financial literacy are more vulnerable to phishing and scams.

Financial uncertainty is also a result of the sector's exposure to global economic instability and volatile digital currency valuations. The future of FinTech and digital

payments depends on strong security measures, flexible regulations, and ongoing technical development to reduce these dangers.

B. Key Components of FinTech and Digital Payments

The FinTech and digital payments ecosystem consists of three key players: **banks, FinTech companies, and regulators**. Banks continue to play a key role in financial services by offering payment processing, traditional banking infrastructure, and frameworks for regulatory compliance. By creating their own digital services or collaborating with FinTech companies, numerous banks are adjusting to the digital revolution [5]. They provide regulatory experience, security, and customer trust, but they frequently lack the agility of tech-driven startups. FinTech businesses propel advancements in blockchain technology, financing, investments, and payments. These businesses, which include PayPal, Stripe, and Square, use cutting-edge technologies like blockchain and artificial intelligence to provide smooth financial services. To make financial services more accessible, startups in this field frequently place a high priority on user experience, inexpensive transactions, and accessibility.

Consumer protection, stability, and compliance are guaranteed by regulators, such as central banks and financial authorities [6]. Regulations for digital transactions, data security, and anti-money laundering (AML) compliance are established by agencies such as the Financial Conduct Authority (FCA), the U.S. Securities and Exchange Commission (SEC), and the Central Bank of Nigeria. While regulations safeguard consumers, they can also create challenges for innovation due to complex compliance requirements.

Collaboration between these players is essential for a secure, efficient, and inclusive financial ecosystem. Banks, FinTech firms, and regulators must work together to balance innovation with security and regulatory oversight.

C. Threat Landscape in FinTech and Digital Payments

As technology evolves, the danger landscape in FinTech and digital payments keeps changing. With hackers using ransomware, phishing, and data breaches to target payment platforms, cybersecurity threats are still a big worry [7]. Users who have weak authentication mechanisms are more susceptible to identity theft and fraud. Risks related to regulations and compliance present additional difficulties. Governments and financial watchdogs enforce strict regulations, like data privacy and anti-money laundering (AML) rules, which can be expensive and difficult for

FinTech companies to comply with [8]. Heavy fines and harm to one's reputation may result from noncompliance. Another risk is technological vulnerabilities, including software bugs, infrastructure failures, and system downtimes that can disrupt transactions. Over-reliance on cloud computing and third-party providers increases the risk of service outages and data leaks.

Financial fraud, such as chargeback fraud and synthetic identity fraud, is on the rise. Criminals exploit digital payment systems to launder money and evade detection.

Market risks also affect FinTech, including economic downturns, fluctuations in cryptocurrency values, and competition from tech giants. Furthermore, a lack of user awareness makes individuals susceptible to scams.

To mitigate these threats, businesses must invest in strong security measures, AI-driven fraud detection, regulatory compliance, and consumer education to ensure a safer financial ecosystem. Below are some of the threats to online payments.

1. *Cyber Threats:* Cyber threats in FinTech and digital payments are a growing concern as cybercriminals develop more sophisticated attack methods. Phishing attacks remain one of the most common threats, where hackers trick users into revealing sensitive information such as login credentials or payment details through fake emails and websites. Ransomware attacks are another major risk, where cybercriminals encrypt financial data and demand payment for its release [9]. These attacks can cripple payment processors, banks, and FinTech platforms, leading to financial losses and reputational damage.Data breaches pose a serious threat, exposing customer information such as credit card details, personal identification, and transaction history. This stolen data is often sold on the dark web, leading to identity theft and financial fraud. Man-in-the-middle (MITM) attacks occur when hackers intercept and manipulate transactions between users and payment systems, allowing them to steal funds or alter transaction details. Furthermore, malware and trojans infect users' devices to capture keystrokes and access financial accounts. As digital payments become more prevalent, API vulnerabilities in payment gateways and banking apps can also be exploited. To combat these threats, FinTech companies must implement multi-factor authentication, encryption, AI-driven fraud detection, and continuous security monitoring to safeguard financial transactions.
2. *Fraud and Financial Crimes:* Fraud and financial crimes pose significant risks to FinTech and digital payment systems, leading to substantial financial losses and reputational damage. Criminals exploit vulnerabilities in online transactions, digital wallets, and banking apps through various fraudulent schemes [10]. One common type is identity theft, where fraudsters steal personal information to open accounts, apply for loans, or conduct unauthorized transactions. Account takeover fraud (ATO) occurs when cybercriminals gain access to a user's financial account and manipulate transactions. Synthetic identity fraud is another rising threat, where criminals combine real and fake personal details to create fraudulent identities and obtain credit [11]. Payment fraud, including chargeback fraud and card-not-present (CNP) fraud, is widespread in e-commerce and digital payments. Fraudsters use stolen credit card details for unauthorized purchases, leading to financial losses for businesses. Another major financial crime involves the funneling of illegal funds through digital transactions to conceal their origins, known as money laundering. To combat fraud, FinTech companies must implement AI-driven fraud detection, biometric

authentication, and transaction monitoring. Regulatory compliance with anti-money laundering (AML) laws and Know Your Customer (KYC) policies is also essential to protect users and ensure the integrity of digital payment ecosystems.

3. *Inside Threats:* Insider threats pose a significant risk to FinTech and digital payment systems, as employees, contractors, or business partners with access to sensitive financial data can intentionally or unintentionally compromise security. These threats are particularly dangerous because insiders often bypass traditional security measures. One type is malicious insiders, where employees or partners intentionally misuse their access to steal funds, leak confidential data, or manipulate transactions for personal gain. Unhappy employees may engage in sabotage, while others may sell user data to cybercriminals. Negligent insiders pose another risk, often due to human error. Employees may fall for phishing scams, misconfigure security settings, or mishandle sensitive data, unintentionally exposing financial systems to breaches. Furthermore, third-party risks arise when vendors or contractors with access to payment systems fail to follow security best practices, making them weak links in cybersecurity. To mitigate insider threats, companies should implement role-based access controls (RBAC), multi-factor authentication (MFA), behavioral monitoring, and strict data access policies [12]. Regular employee training and conducting background checks on staff with privileged access can also help prevent insider-related fraud and security breaches.

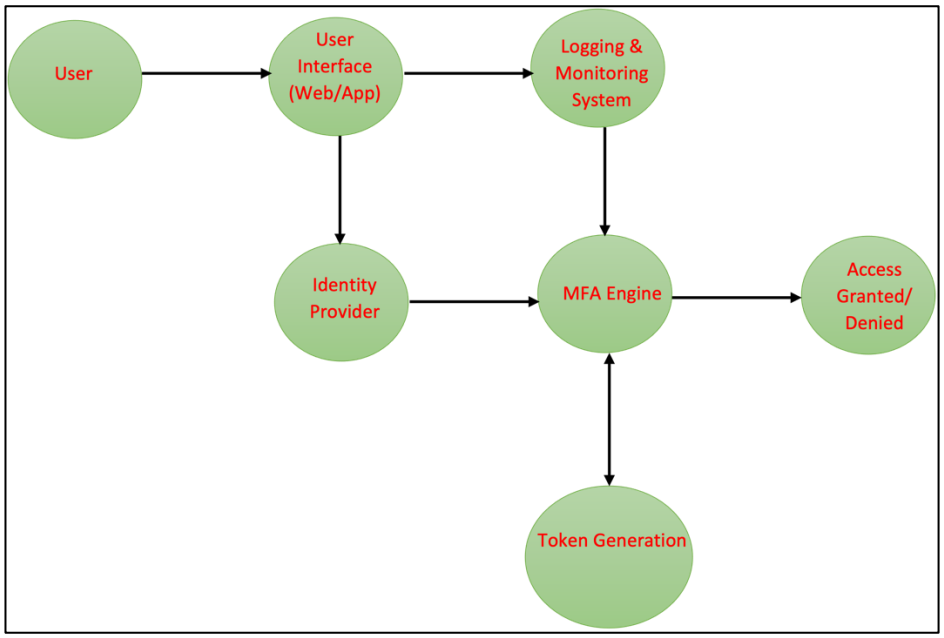

Fig. 1. Multi-factor Authentication

Encryption plays a vital role in securing digital transactions and protecting sensitive financial data from cyber threats. By implementing strong encryption protocols, FinTech companies and payment service providers ensure that user credentials, payment details, and transaction information remain confidential and protected from unauthorized access.

End-to-end encryption (E2EE) is a widely used security mechanism that ensures data remains encrypted from the sender to the receiver, preventing interception by third parties. This safeguard is particularly crucial in digital payments, where sensitive information such as credit card numbers and banking credentials must be protected from eavesdropping and data breaches. Secure communication channels, including TLS (Transport Layer Security), further enhance security by encrypting data in transit.

Tokenization is another critical security method that replaces sensitive data with randomly generated tokens. Unlike encryption, where data is transformed into ciphertext and can be decrypted, tokenization completely replaces the original information, making it useless to attackers. Cryptographic methods such as hashing, asymmetric encryption, and digital signatures further enhance security by ensuring data integrity and verifying transaction authenticity.

By integrating these encryption and cryptographic techniques, FinTech firms can prevent data breaches, mitigate fraud, and ensure secure communication across digital payment systems.

D. Social Engineering and Attacks

Social engineering is not about sophisticated technical hacking; it manipulates human behavior to breach security [13]. As technology advances, the complexity of technical cyberattacks increases, making them harder to execute. However, social engineering remains highly effective, using deception to exploit human vulnerabilities and bypassing even the most advanced security systems. Attackers leveraging this tactic can infiltrate networks, bypass firewalls, implant malware, or establish backdoor access. The key to social engineering lies in exploiting cognitive biases and human error, rather than technical flaws, to obtain sensitive information or access. Social engineering is defined as one of

the simplest ways to gather information about a target by exploiting human weaknesses present in every organization. Attackers use this technique to manipulate individuals into revealing confidential information, which is then used to compromise the organization's security [14]. This type of attack makes human vulnerability a critical weak point in cybersecurity.

While social engineering is often considered low-tech, it is highly successful because it preys on the psychological flaws of individuals. Security technologies may strengthen system defenses, but human factors remain the most exploitable link. In essence, attackers use social engineering to circumvent security measures by deceiving human insiders, making it a powerful tool in modern cyberattacks.

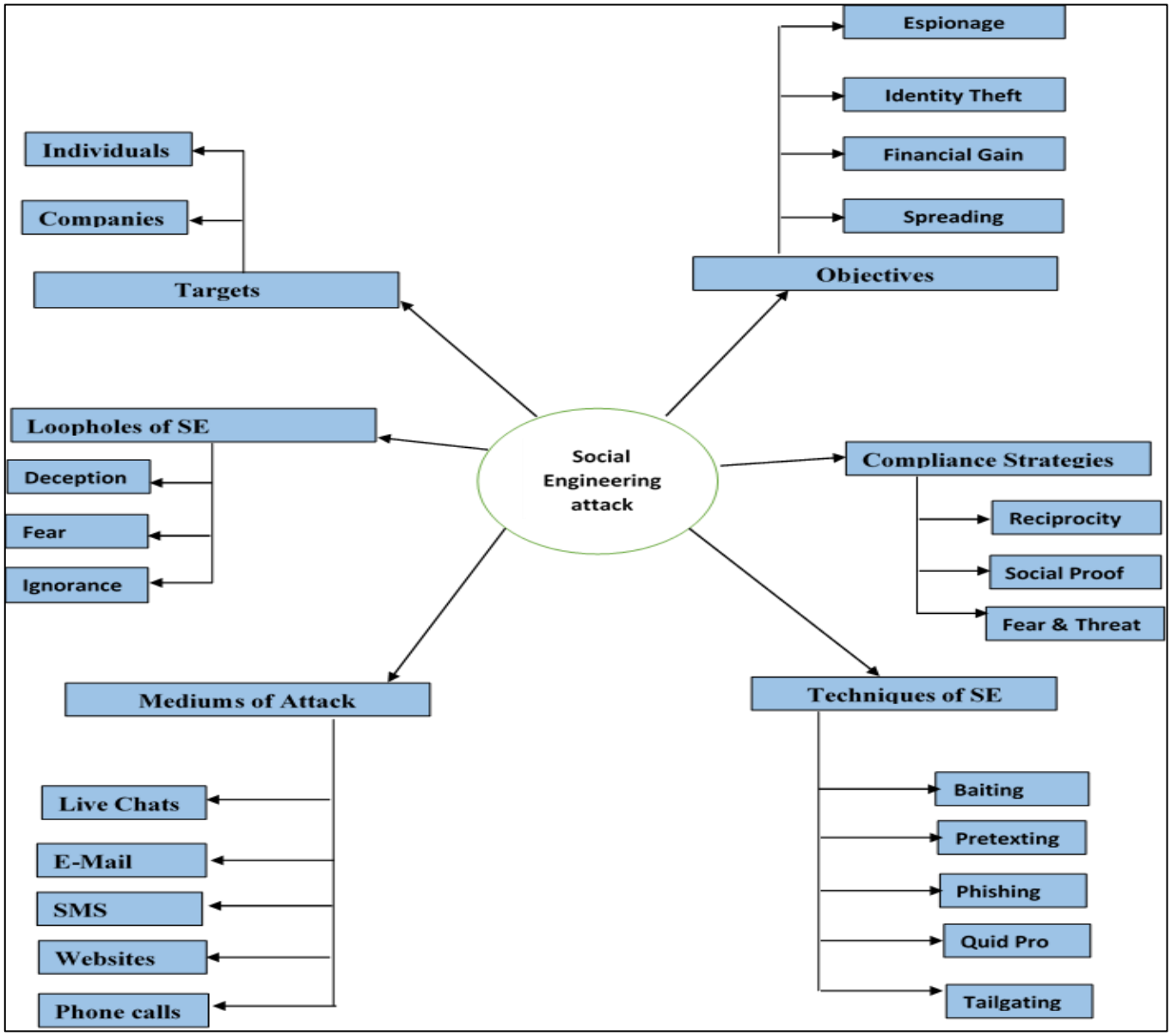

Fig. 2. Social Engineering [13]

E. Regulatory Compliance & Standards in FinTech and Digital Payments

Regulatory compliance is essential for ensuring security, transparency, and trust in FinTech and digital payment ecosystems. Governments and financial authorities impose strict regulations to prevent fraud, money laundering, and data breaches while ensuring consumer protection [15].

Globally, compliance frameworks such as AML (Anti-Money Laundering), KYC (Know Your Customer), GDPR (General Data Protection Regulation), and PCI-DSS (Payment Card Industry Data Security Standard) set guidelines for identity verification, data privacy, and secure transactions. The Financial Action Task Force (FATF) also provides international standards for combating financial crimes.

In Nigeria, regulatory bodies like the Central Bank of Nigeria (CBN), the Nigeria Financial Intelligence Unit (NFIU), and the Securities and Exchange Commission (SEC) oversee FinTech operations. CBN's Regulatory Framework for Open Banking promotes data security, while its AML/CFT (Anti-Money Laundering and Counter Financing of Terrorism) guidelines help combat financial fraud. The National Information Technology Development Agency (NITDA) enforces data protection laws similar to GDPR.

FinTech firms must comply with these regulations by implementing strong identity verification measures, secure transaction protocols, and regular compliance audits [16]. Adherence to these standards not only ensures legal operations but also enhances user trust and financial system stability in Nigeria and beyond.

F. Digital Currency

Digital Currency is a new concept popularized with the rapid rise of the Internet. CBDC (Central Bank Digital Currency) define Digital Currency as a form of a country's fiat currency. Instead of printing paper currency or minting coins, the central bank issues electronic tokens. Digital currency can also be referred to as virtual currency, a currency used in a virtual world that can indirectly hold value in real life [17]. Meanwhile, the introduction of digital currency produces various associated challenges in regulation, tracking of funding and taxing, purchasing by individuals, etc.

Typical example of digital currency is Crypto currency. By definition, Crypto currency is the name given to a system that uses cryptography to allow the secure transfer and exchange of digital tokens in a distributed and decentralized manner [18]. According to Ametrano, (2014), it is a currency that can be transferred instantly between any two parties, using the Internet infrastructure and cryptographic security with no need for a trusted third party. Its value is not backed by any single government or organization. Crypto currency uses distributed ledger, or blockchain, technology to enable a secure transaction [19].

It is a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of carrying physical money around and exchanged in the real world, crypto currency payments exist purely as digital entries to an online database describing specific transactions. When you transfer crypto currency funds, the transactions are recorded in a public ledger [20]. From the definitions above, crypto currency can simply be described as a digital currency that uses cryptography for secure financial transactions, it operates a decentralized, secured system without a central authority, such as a government or bank.

The main idea behind crypto currencies is to provide a fast way to transfer funds globally, with minimal transaction costs and a certain amount of privacy in which the sender and receiver are always anonymous while being independent of a third party to handle the transactions. Transactions made with Bitcoin is irreversible; this way, the recipient of the funds is sure they own them for good. Therefore, less trust is needed to ensure the other party is reliable.

G. FinTech and Digital Payments

FinTech and digital payments in Nigeria have transformed nearly all aspects of financial transactions through mobile wallets, digital banks, and cryptocurrency platforms. Here is a brief overview of some of these technologies.

1. *Opay:* Founded in 2018, OPay is a leading fintech platform in Nigeria, offering mobile payments, money transfers, bill payments, and loans. Its app provides a seamless way for users to send money, pay for utilities, and shop online. OPay also supports businesses with merchant payment solutions, helping to streamline transactions. With a growing user base, it plays a significant role in promoting cashless payments and financial inclusion across Nigeria. Also, OPay has expanded its services to include savings by introducing Owallet.
2. *fintech:* The fintech, introduced by the Central Bank of Nigeria (CBN) in 2021, is a blockchain-based digital currency designed to complement the physical Naira. It is centrally controlled, backed by the Naira (1:1), and requires an fintech wallet for transactions. The currency enables instant, low-cost transactions across mobile devices, web browsers, and POS terminals. fintech aims to enhance financial inclusion, reduce cash management costs, boost tax revenue collection, and support economic growth through a secure, efficient digital payment system. Unlike cryptocurrencies, which are decentralized and volatile, fintech is stable and regulated by the CBN.Despite banning cryptocurrency transactions in 2021 due to concerns about financial fraud, the CBN acknowledges that crypto and fintech can coexist—fintech for everyday transactions and crypto for cross-border payments and remittances. The fintech wallet functions like a bank account but operates separately, providing Nigerians with a safe, digital alternative for financial transactions.

Fig. 3. Objectives of the fintech

3. *Flutterwave:* Flutterwave, founded in 2016 by a team of Nigerian entrepreneurs and technologists, is a financial technology company that provides digital payment infrastructure for businesses and individuals across Africa. The company was established to address the fragmented and often unreliable payment systems on the continent and to make financial transactions simpler, faster, and more secure. Since its inception, Flutterwave has become one of Africa's leading payment service providers. The platform enables merchants to accept payments

in over 150 currencies through various channels, such as debit and credit cards, bank transfers, mobile money, and USSD. This wide range of payment options helps businesses reach more customers, both locally and globally. Flutterwave supports seamless integration with international payment systems, which simplifies cross-border transactions and opens up African markets to global trade. According to [21], platforms like Flutterwave have played a significant role in improving financial accessibility and infrastructure in emerging markets. In addition to core payment processing, Flutterwave offers tailored products for different user needs. One such service is Barter, a digital wallet that allows individuals to send and receive money, create virtual dollar cards, and pay for services such as subscriptions and online shopping. Another product, Flutterwave Store, helps small and medium-sized businesses create online storefronts without the need for coding or extensive technical knowledge. This feature became particularly popular during the COVID-19 pandemic when many physical businesses shifted to online platforms. Flutterwave also provides a robust and developer-friendly API that enables software developers to embed secure and reliable payment solutions directly into web and mobile applications. This flexibility makes it easy for businesses of all sizes to integrate financial services without building them from scratch. By offering these services, Flutterwave contributes to increasing financial inclusion in Africa, where many people and businesses remain underserved by traditional banking systems. The platform reduces the barriers to entry for entrepreneurs and small businesses, enabling them to participate more actively in the digital economy. Furthermore, by facilitating easier access to global payment networks, Flutterwave helps African businesses scale beyond local markets.

4. *Apple Pay:* Apple Pay is a mobile payment and digital wallet service developed by Apple. Launched in 2014, it enables users to make secure, contactless payments using iPhones, iPads, Apple Watches, and Macs. It works with NFC technology, allowing payments at retail stores, apps, and websites. Apple Pay integrates with bank cards and supports tokenization, ensuring secure transactions without sharing card details. It is widely accepted globally and offers features like peer-to-peer payments via Apple Cash. With built-in encryption and Face ID or Touch ID authentication, Apple Pay provides a fast, secure, and convenient way to make digital payments worldwide.
5. *Stablecoins:*Stablecoins are a type of cryptocurrency designed to maintain a stable value by pegging their price to a reserve asset like fiat currency, commodities, or a basket of assets. Unlike traditional cryptocurrencies, which are highly volatile, stablecoins offer price stability, making them useful for payments, remittances, and store of value. There are three main types of stablecoins: Fiat-backed (e.g., USDT, USDC), Crypto-backed (e.g., DAI), and Algorithmic stablecoins, which use smart contracts to regulate supply. Stablecoins play a crucial role in decentralized finance (DeFi) by enabling seamless trading, lending, and cross-border transactions while reducing exposure to market fluctuations.
6. *Chipper Cash:* Chipper Cash is a fintech company that facilitates cross-border payments and remittances across Africa. Founded in 2018, it enables individuals and businesses to send and receive money instantly across multiple countries with low fees. The platform supports mobile wallets, bank transfers, and card payments, making digital transactions more accessible. Chipper Cash also offers virtual cards for online payments, cryptocurrency trading, and business payment solutions. It provides a fast, secure, and cost-effective alternative to traditional banking, promoting financial inclusion across the continent. With millions of users, the platform is transforming the way Africans handle money, making seamless cross-border transactions a reality for individuals and businesses alike.

H. Vulnerabilities in FinTech and Digital Payment Systems

FinTech and digital payment systems face multiple security challenges. Weak authentication mechanisms make accounts susceptible to unauthorized access. Poorly secured API integrations expose sensitive financial data to cyber threats. Data breaches and leakage risks remain significant concerns, potentially leading to financial losses and identity theft [22]. Regulatory compliance gaps create loopholes that cybercriminals can exploit, especially when financial institutions fail to meet evolving security standards. Insider threats pose another risk, as employees with access to sensitive information may misuse it for personal gain or inadvertently compromise security. To mitigate these risks, strong authentication protocols, robust API security measures, and stringent regulatory adherence are essential [23]. Financial institutions must also implement continuous monitoring and employee training to detect and prevent insider threats. Strengthening cybersecurity frameworks in FinTech and digital payment systems is crucial to ensuring data integrity, user trust, and the long-term stability of financial transactions.

I. Security Technologies and Best Practices

1. *Authentication & Authorization:* Implementing Multi-Factor Authentication (MFA) enhances security by requiring multiple verification factors. Biometric security, such as fingerprint or facial recognition, provides an additional layer of protection [3]. Passwordless authentication, using cryptographic keys or biometric data, reduces reliance on traditional passwords, minimizing phishing risks.
2. *Data Protection:* End-to-end encryption (E2EE) ensures data remains protected during transmission,

preventing unauthorized interception. Tokenization replaces sensitive data with unique tokens, reducing exposure to breaches. Secure cloud storage, combined with database encryption, safeguards information against unauthorized access. Enforcing strong access controls and real-time monitoring further enhances security. By integrating these technologies and best practices, organizations can strengthen cybersecurity defenses, mitigate risks, and protect user data from evolving threats.

3. *Fraud Prevention:* One key factor of cybersecurity is fraud prevention, especially in industries like banking, e-commerce, and finance where fraudulent activity can result in large financial losses as well as harm to an organization's reputation [24]. By spotting patterns and irregularities that point to questionable activity, artificial intelligence (AI) and machine learning (ML) have emerged as crucial instruments in the fight against fraud in recent years.

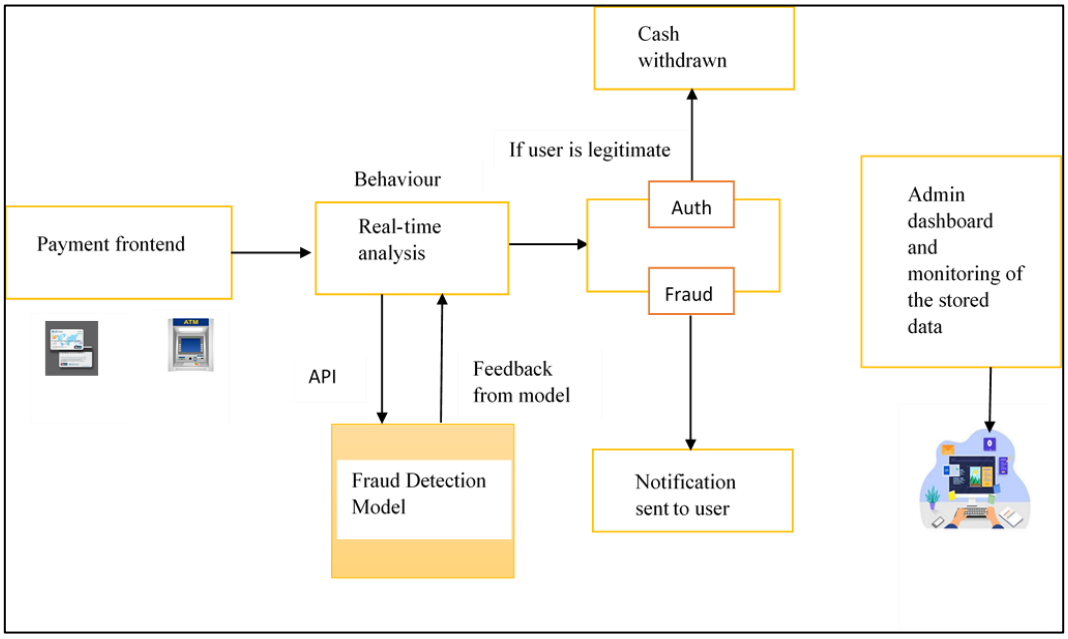

Fig. 4. Fraud Detection Model [24]

J. Future Trends and Innovations in FinTech Security

The financial technology sector is rapidly evolving, integrating advanced security measures to combat cyber threats. Artificial Intelligence (AI) and Machine Learning (ML) play a crucial role in detecting fraudulent activities, analyzing transaction patterns, and automating threat responses in real-time [25].

Quantum cryptography is emerging as a next-generation security solution, offering ultra-secure encryption for financial transactions, making it nearly impossible for cybercriminals to decrypt sensitive data. The Zero-Trust Security Model is transforming digital banking by enforcing strict identity verification at every access point, reducing the risk of unauthorized access and insider threats [26].

Decentralized identity verification leverages blockchain technology to give users control over their digital identities, minimizing data breaches and identity theft. As cyber threats evolve, these innovations will redefine FinTech security, ensuring safer financial transactions, stronger authentication, and enhanced data protection across digital payment platforms.

K. Some Security bridges in FinTech and Digital Payments

1. *Flutterwave Security Breaches:* Flutterwave, one of Nigeria's leading fintech companies, has suffered multiple security breaches, raising concerns about its cybersecurity framework. In February 2023, the company reported an unauthorized transfer of ₦2.9 billion from its accounts. Hackers exploited vulnerabilities in Flutterwave's system, moving funds into various bank accounts. The incident triggered an investigation, leading to the freezing of several accounts suspected to have received the stolen funds. In April 2024, Flutterwave experienced an even larger breach. This time, ₦11 billion was illicitly transferred across multiple accounts. The attackers strategically moved the money in small amounts, making it harder for fraud detection systems to flag the transactions immediately. Reports suggest that the breach may have involved insider collaboration or sophisticated hacking techniques that bypassed Flutterwave's security protocols. Following these breaches, concerns about weak internal controls, fraud monitoring gaps, and regulatory compliance have grown. Critics argue that the repeated attacks indicate systemic security flaws that could expose customer funds to future risks. Regulators and financial institutions have urged Flutterwave to enhance its cybersecurity measures, while customers remain wary of potential vulnerabilities in Nigeria's rapidly expanding fintech ecosystem.
2. *Hope Payment Service Bank Incident:* In October 2024, Hope Payment Service Bank, a digital-first financial institution in Nigeria, suffered a massive

security breach, resulting in the unauthorized transfer of ₦10 billion. Cybercriminals orchestrated a sophisticated attack, exploiting vulnerabilities in the bank's system to siphon funds into multiple accounts. The scale of the fraud quickly drew the attention of financial regulators and law enforcement agencies. Following an investigation, the Federal High Court ordered the freezing of 818 accounts suspected of receiving and distributing the stolen funds. The move aimed to prevent further withdrawals and trace the masterminds behind the cyber heist. While details of the attack remain unclear, cybersecurity analysts suspect that the breach involved a mix of social engineering, insider threats, and weaknesses in transaction monitoring systems. The incident has intensified discussions around Nigeria's fintech security landscape, emphasizing the need for stricter regulatory oversight, stronger fraud detection mechanisms, and enhanced cybersecurity frameworks to prevent future breaches.

III. METHODOLOGY

The architecture of the proposed security assessment model is in four layers. They are Data Collection layer, Data Preprocessing Layer, Data Presentation and Result layer. The layers are further explained below:

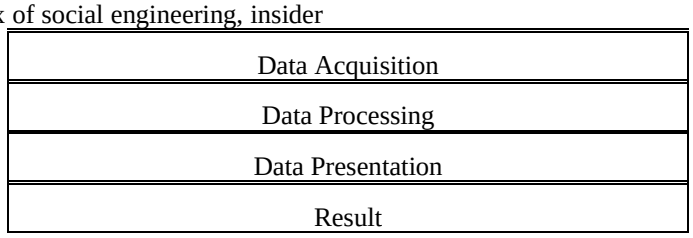

Fig. 5. Architectural Model

Data Collection: Data Collection is the data gathered from survey respondents and Google sources.
Data Preprocessing: This step involves preparing the collected data for analysis using the assessment model. Once the data is collected, it undergoes pre-processing through a data normalization module. This process handles data that may include large values, small values, and different data types.
Data Presentation: In this step, the analyzed data is presented in a tabular format to facilitate decision-making.
Result: At this stage, the presented results are utilized by the security model to make informed decisions. The detected outcomes also contribute to updating the knowledge of the fintech and digital payment software developers, enabling them to enhance security measures and be more security-conscious.

A. Demographic Information

Table 1 shows the Bio-data information of respondents, Sex of Respondent.

Table 1: Bio-data information based on Gender Respondent

Variable	Respondents	Percentage (%)
Male	65	81.25
Female	20	18.75
Total	85	100

The information shows that 65 of the respondents representing 81.25% were male, while 20 respondents representing 18.75%, were female. This implies that males are more in number than females. Table 2 depicts the marital status of respondents. The table indicated that 25 respondents representing 29.41% are married, 50 respondents representing 58.82% are Single, while 10 respondents representing 11.77% are divorced. This indicated that those that are Single are more in number.

Table 2: Marital Status of Respondent

Variable	Respondents	Percentage (%)
Married	25	29.41
Single	50	58.82
Divorced	10	11.77
Total	85	100

Table 3 show that 27 respondents representing 31.73% are between the ages of 15-24 years, 25 respondents representing 29.41% are between the ages of 25-34 years, 20 respondents representing 23.52% are between the ages of 35-44 years while 13 respondents representing 15.29% are ages of 45 and above years.

Table 3: Age Range of Respondents

Variable	Respondents	Percentage (%)
15-24years	27	31.73
25-34years	25	29.41
35-44	20	23.52
45 and Above	13	15.29
Total	85	100

Table 4 represent information on educational qualification of respondents.

Table 4: Educational Qualification of Respondents

Variable	Respondents	Percentage (%)
FLSC	13	15.29
WAEC/GCE	17	20
HND/BSc	25	29.42
Master Degree	20	23.53
Others	10	11.76
Total	85	100

The table shows that 13 respondents representing 15.29% are FLSC Holders , 17 respondents representing 20% are WACE/GCE Holders , 25 respondents representing 29.42%

are HND/BSc Holders,20 respondents representing 23.53% are Master's Degree Holders,10 respondents representing 11.76% are other Degree Holders . This shows that those with HND/BSc. Holders have the highest percentage of respondents in the labour market.

Table 5: Religion of Respondent

Variable	Respondents	Percentage (%)
Christian	46	54.1
Moslem	25	29.4
Pagan	14	16.5
Total	85	100

The above table 5 shows that 46 respondents representing 54.1% are Christian, 25 respondents representing 29.4% are Moslem, 14 respondents representing 16.5% are Pagan. This indicated that Christians are more in the target audience.

B. Analysis of Responses to the Research Questions

Table 6 (question 1): Is fraud prevention lectures given in the school and market places?

Variable	Respondents	Percentage (%)
Yes	68	80
No	15	17.65
I don't know	2	2.3
Total	85	100

The above table 6 show that 68 respondents representing 80% say Yes Fraud Prevention lectures is given in the school 15 respondents representing 17.65% says No, 2 respondents representing 2.3% says I don't know. This indicated that fraud prevention often lecture fraud prevention lectures in the school.

Table 7 (questions 2): Can you make payment with fintech Application?

Variable	Respondents	Percentage (%)
Yes	53	66.25
No	13	12.5
I don't know	19	21.25
Total	85	100

The above table 7 show that 53 respondents representing 66.25% say yes they can make payment with fintech app, 13 respondents representing 12.5% says No, while 19 respondents representing 21.25% say I don't know. This indicated that market women, professionals and student can make payment with fintech Application.

Table 8. (Question 3): Is the level of fraud prevention in the application up to 50%?

Variable	Respondents	Percentage (%)
Yes	70	82.45
No	9	10.58
I don't know	6	7.06
Total	85	100

The above table 8 show that 70 respondents representing 82.45% say yes that the level of safety compliance for fraud prevention are up to 50%, 9 respondents representing 10.58% say No while 6 respondents representing 7.06% say I don't Know that the level of fraud prevention 50%, .This indicated that the level of fraud prevention in the fintech application is up to 50%.

Table 9 (question 4): Are there any OTP mechanism to prevent fraud activities?

Variable	Respondents	Percentage (%)
Yes	62	72.94
No	15	17.65
I don't know	8	9.41
Total	85	100

The above table 9 show that 62 respondents representing 72.94% say yes there is OTP security mechanism while registration is ongoing in the fintech application, 15 respondents representing 17.65% say No there are OTP security mechanism while registration is ongoing in the fintech application, 8 respondents representing 9.41% say I don't know if there OTP security mechanism while registration is ongoing in the fintech application. This indicate that there are OTP security mechanism while registration is ongoing in the fintech application.

Table 10 (question 5): Are there trained ethical hackers working and updating the fintech and digital application?

Variable	Respondents	Percentage (%)
Yes	58	68.24
No	15	17.65
I don't know	12	14.11
Total	85	100

The above table 10 shows that 58 respondents representing 68.24% say yes there are trained ethical hackers, 15 respondents representing 17.65% say No there are no trained ethical hackers, 12 respondents representing 14.11% say I don't know if there are trained ethical hackers. This indicated that there are trained ethical hackers working for the federal government to prevent hackers intrude the fintech application.

Table 11 (Question 6): How would you rate the fraud preventive measures in the fintech application, is it high or low?

Variable	Respondents	Percentage (%)
Yes	66	77.7
No	15	17.5
I don't know	4	4.8
Total	85	100

The above table 11 shows that 66 respondents representing 77.7% say yes the fraud preventive measures in the fintech application is high 15 respondents representing 17.5% say No the fraud preventive measures in the fintech application is not high but low, 4 respondents representing 4.8% says I don't know How would you rate the fraud preventive measures in the fintech application is it high or low. This indicated that the fraud preventive measures in the fintech application is high.

Table 12 (Question 7): Are there frequent update on the app on playstore and app store?

Variable	Respondents	Percentage (%)
Yes	44	52
No	16	18.9
I don't know	25	29.4
Total	85	100

The above table 12 shows that 44 respondents representing 52% say yes. There are frequent upgrade and update on the fintech app on cross-platforms, 16 respondents representing 18.9% say No there are no update on the fintech application while 25 respondents representing 29.4% says I don't know if there are frequent upgrade and update on the application. This indicated there is frequent upgrade and update on the application.

Table 13 (Question 8): Have there ever being technical glitch in the fintech application?

Variable	Respondents	Percentage (%)
Yes	10	12
No	68	80
I don't know	7	8
Total	85	100

The above table 13 show that 10 respondents representing 12% say yes there are technical glitch in the fintech app, 68 respondents representing 80%, say No there have never being while 7 respondents representing 8% says I don't know if there are technical glitch. This indicated that the level technical problems influence the usage of the app.

Table 14 (Question 9): Are no signs visibly displayed in the app when a third party tried to login?

Variable	Respondents	Percentage (%)
Yes	16	18
No	50	59
I don't know	19	23
Total	85	100

The above table 14 show that 16 respondents representing 18% say yes no signs is visibly displayed in the app when a third party login, 50 respondents representing 59% says No, no visibly displayed sign when a third party login while 19 respondents representing 23% says I don't know if signs are visibly displayed when third party login. This indicated that signs are not visibly displayed in the app when third party login.

Table 15 (question 10): Do fintech app allow facial recognition in the authentication process?

Variable	Respondents	Percentage (%)
Yes	9	10.5
No	70	82.4
I don't know	6	7.1
Total	85	100

The table 15 above show that 70 respondents representing 82.4% say no there is facial recognition when login in process, 9 respondents representing 10.5%, say yes there are no facial recognition when registration in progress While 6 respondents represent 7.1% says I don't Know if there is facial recognition in the fintech application. This indicated that there is no facial recognition mechanism or technique when login or registration in progress.

Table 16: Result Model Table

Sample Variable	Level of Education	OPT Mechanism	Frequent Update	Technical Glitch	Level of Fraud Prevention
Yes		Yes	Yes		
No				No	
High	High				High
Low					

The Result Model table reveals the collated and analyzed data of correspondents, highlighting the Fraud Risk Assessment Model used in the fintech application. The analysis of the Result Model indicates a high level of education among the surveyed individuals. Additionally, the fintech application incorporates the OPT mechanism and receives regular updates on both Playstore and Appstore. It is noteworthy that technical glitches are infrequent, and the application implements robust fraud prevention measures.

In order to obtain the expected frequency we divided the total frequencies for each response by the number of rows.
Grand Total = 85
Number of Rows = 3

Expected Frequency (fe) $\frac{85}{3}$= 28.33

fe =28.33
Chi-square formula;
(fo — fe)2/ fe = chi-square
fo Observed Frequency
fe Expected Frequency

Table 17: The calculation of the chi-square is shown in the table below

Variable	Fo	Fe	Fo-fe	$(fo-fe)^2$	$(Fo-fe)^2/fe$
Yes	68	28.33	39.67	1,573.7	**55.55**
No	15	28.33	-13.33	177.69	**6.27**
I don't know	2	28.33	-26.33	693.27	**24.47**
Total	85				**86.29**

Critical value 5.991
Cal. value 86.29
The computed value of the X2 is (86.29). To find the critical value of X2, we used 5% (0.05) as our level of significance.
The degree of freedom is calculated by dfr – 1
Where;
df = Degree of Freedom
r = Number of Rows
c = Number of column
Where
df = (3- 1) (2-1) (2)(1)
(2)
Df = 2

Using the chi-square table to calculate the critical value, we look for two (2) under the df column and 0.05 along the level of significance. From the X2 table, our critical value is 5.991.

Decision
Since the calculated value (86.29) is greater than the critical value (5.991), we therefore reject the alternative hypothesis and accept the null hypothesis (H0) There may be fraud prevention lectures given in the school. IT professionals, students, and market women can make use of fintech application for payment and reception of cash. The above hypothesis was tested with data contains in table 4.7(question 7). In order to obtain the expected frequency we divided the total frequencies for each response by the number of rows.
Grand Total 85
Number of Rows = 3
Expected Frequency (fe) $\frac{85}{3}$= 28.33
fe = 28.33
Chi-square formula;
(fo fe)2
Fe
X2 = chi-square fo = Observed Frequency fe = Expected Frequency
The calculation of the chi-square is shown in the table below:
Critical Value 5.991
Cal Value = 32.84
The computed value of the X2 is (32.84). To find the critical value of X2, we used 5% (0.05) as our level of significance.
The degree of freedom is calculated by
Dfr- 1
Where;
= Degree of Freedom
= Number of Rows Number of column Where
df = (3 - 1) (2-1) (2)(l)
(2)
Df = 2
Using the chi-square table to calculate the critical value, we look for two (2) under the df column and 0.05 along the level of significance. From the X2 table, our critical value is 5.991.

Table 18: The calculation of the chi-square

Variable	Fo	Fe	Fo-fe	$(fo-fe)^2$	$(Fo-fe)^2/fe$
Yes	53	28.33	24.67	608.61	21.48
No	13	28.33	-15.33	235.01	8.3
I don't know	19	28.33	-9.33	87.05	3.07
Total	85				32.84

Decision
Since the calculated value (32.84) is greater than the critical value (5.991), we therefore reject the alternative hypothesis and accept the null hypothesis (H02) which states that professionals, market women and student can operate the fintech application.
Can fraud preventive training test the level of fraud risk assessment in the fintech app. In order to obtain the expected frequency we divided the total frequencies for each response by the number of rows.
Grand Total 85
Number of Rows = 3
Expected Frequency (fe) $\frac{85}{3}$= 28.33
fe = 28.33
Chi-square formula;
(fo - fe)2
fe
X2 chi-square
fo Observed Frequency fe = Expected Frequency
The calculation of the chi-square is shown in the table below:
The computed value of the X2 is (30.58). To find the critical value of X2, we used 5% (0.05) as our level of significance.
The degree of freedom is calculated by
df = r – 1 Where;
df = Degree of Freedom r Number of Rows c=Number of column Where df = (3-l)(2-1)
(2)(1)
(2)
Df = 2
Using the chi-square table to calculate the critical value, we look for two (2) under the df column and 0.05 along the level of significance. From the X2 table, our critical value is 5.991.

Table 19: The calculation of the chi-square

Variable	Fo	Fe	Fo-fe	$(fo-fe)^2$	$(Fo-fe)^2/fe$
Yes	10	28.33	-18.33	335.99	11.86
No	68	28.33	39.67	1,573.7	55.54
I don't know	7	28.33	-21.33	454.97	16.06
Total	85				83.46

Decision

Since the calculated value (83.46) is greater than the critical value (5.99 1), we therefore the reject the alternative hypothesis and accept the null hypothesis (H03) which stated that Can fraud preventive training test the level of fraud risk assessment in the fintech app.

fintech app allows BVN and other personal number verification before transactions can take place?

The above hypothesis was tested with data contains in table 11(question 11). In order to obtain the expected frequency we divided the total frequencies for each response by the number of rows.

Grand Total 85

Number of Rows = 3

Expected Frequency (fe) $\frac{85}{3}$= 28.33

fe = 28.33

Chi-square formula;

(fo -fe)2

fe

chi- square

fo = Observed Frequency

fe = Expected Frequency

The calculation of the chi-square is shown in the table below:

The computed value of the X2 is (83.46). To find the critical value of X2, we used 5% (0.05) as our level of significance.

The degree of freedom is calculated by df = r – 1

Where;

df Degree of Freedom r = Number of Rows c=Number of column Where df = (3-l) (2-1) = 2

(2) (1)

(2}

Df = 2

Using the chi-square table to calculate the critical value, we look for two (2) under the df column and 0.05 along the level of significance. From the X2 table, our critical value is 5.991.

Table 20: The calculation of the chi-square

Variable	Fo	Fe	Fo-fe	$(fo-fe)^2$	(Fo-fe)2/fe
Yes	71	28.33	24.67	608.61	21.48
No	7	28.33	-15.33	235.01	8.3
I don't know	7	28.33	-15.33	235.01	8.3
Total	85				38.08

Decision

Since the calculated value (38.08) is greater than the critical value (5.991), we therefore reject the alternative hypothesis and accept the null hypothesis which stated that fintech app allows BVN and other personal number verification before transactions can take place

Do fintech app has an end-to-end encryption techniques

The above hypothesis was tested with data contains in table 17(question 17)

Do fintech app has an end-to-end encryption techniques?

In order to obtain the expected frequency we divided the total frequencies for each response by the number of rows.

Grand Total 85

Number of Rows 3

Expected Frequency (fe) = $\frac{80}{3}$ = 28.33

fe = 28.33

Chi-square formula;

$\frac{(fo - fe)^2}{fe}$

chi-square

fo Observed Frequency

fe Expected Frequency

The calculation of the chi-square is shown in the table below:

The computed value of the X^2 is (87.19). To find the critical value of X^2, we used 5% (0.05) as our level of significance.

The degree of freedom is calculated by df = r – 1

Where;

df = Degree of Freedom

r = Number of Rows c Number of column

Where

df = (3-l) (2-l) = 2

(2) (l)

(2)

Df = 2

Using the chi-square table to calculate the critical value, we look for two (2) under the df column and 0.05 along the level of significance. From the X^2 table, our critical value is 5.991.

Table 21: The calculation of the chi-square

Variable	Fo	Fe	Fo-fe	$(fo-fe)^2$	$(Fo-fe)^2/fe$
Yes	70	28.33	42.62	1,736.39	61.29
No	7	28.33	-15.33	235.01	8.3
I don't know	6	28.33	-22.33	498.63	17.60
Total	85				87.19

Decision

Since the calculated value (87.19) is greater than the critical value (5.991), we therefore reject the alternative hypothesis and accept the null hypothesis ($H0_5$) which states that fintech app has an end-to-end encryption techniques.

Discussion of Data

Based on the findings revealed from the study, the table 1 showed that 65 of the respondents representing 81.25% were male while 20 respondents representing 18.75% were female. This implies that male are more in number than the female in the selected group of people under study and have the highest percentage of 81.25% respondents.

The table 2 showed that 25 respondents representing 29.41% are married, 50 respondents representing 58.82%are single, while 10 respondents representing 11.77% are divorced. This indicated that those that are Single have the highest percentage of respondents of 58.82% under study in responding to the questionnaire.

The table 3 show that 27 respondents representing 31.73% are between the ages of 15-24 years, 25 respondents representing 29.41% are between the ages of 25-34 years, 20 respondents representing 23.52% are between the ages of 35-44 years while 13 respondents representing 15.29% are ages of 45 and above years. This indicated that those between the ages of 15-24 years are more in number in the survey. The checklist showed a list of fraud and using the fraud assessment matrix, fraudulent activities were ranked based on their likelihood of occurrences and severity.

Table 22: Security Assessment Matrixes

Increasing Likelihood	5	**Happens every day in our Bank**	**5**	**10**	**15**	**20**	**25**	**30**
	4	Happened several times per year in our Bank.	4	8	12	16	20	24
	3	Incident has occurred in our Bank	3	6	9	12	15	18
	2	Heard of incident in the Bank	2	4	6	8	10	12
	1	Never heard of incident in the Bank.	1	2	3	4	5	6
Consequence		Humans	No Effect	Slight trust issue	Minor trust issue	Major trust issue	Fraud	Multiple Fatalities
		App error	No App crash	Slight crash	Minor glitches	Localized error	Major error	Extensive error
	Severity		1	2	3	4	5	6

Table 23: Fraud Rating and Action Priority Key

Fraud level	Action priority
Very high fraud	Immediate action to be completed (required urgently)
High fraud	Action to be completed promptly preferably within 3 months
Medium fraud	Action to be completed, preferably within 6 months (strongly recommended)
Low fraud	Actions to be completed within 12 months (recommended)/No action required.

Table 24: Fraud prevention Performance for awareness campaign

	Authentication	Invasion Risk	Severity	Likelihood	Fraud Rating	% Fraud Rating
1.	Facial recognition	Not Vulnerable	No breach (2)	3	6(M)	20
2.	Password	Not Vulnerable	No breach (2)	4	8(M)	26.7
3.	Email	Not Vulnerable	No breach (2)	3	6(M)	20
4.	Loss of smartphone	vulnerable	Fatality breach (5)	2	10(M)	33.3
5.	Leaked password	Vulnerable	Slight breach(2)	4	8(M)	26.7
6.	No OTP	Vulnerable	Slight effect (2)	3	6(M)	20
7.	Improper display of OTP	Vulnerable	High risk (3)	3	9(M)	30
8.	Frequent Login	Vulnerable	2	5	10(H)	33.3

Total % Fraud rating 210
Average % Fraud rating = 23.3%
Fraud rating = Likelihood x severity
% risk rating x 100
RAM = 6 x 5
Those who are vulnerable
Professionals, Students, Market Women
Numbers employed: Professionals = 30
Student = 500
Market Women = 15
Total 590 persons

IV. Recommendation And Conclusions

To reduce unauthorized access, FinTech firms should implement Multi-Factor Authentication (MFA) using combinations such as device-based verification, biometrics (e.g., fingerprint or facial recognition), and passwordless login options (e.g., magic links or hardware security keys). Biometric systems should include fallback mechanisms and anti-spoofing measures to enhance reliability.

For API security, companies should adopt OAuth 2.0 for secure authorization, enforce TLS encryption for all communication, and deploy real-time traffic monitoring tools such as API gateways with anomaly detection. Additionally, rate limiting and IP whitelisting can help minimize abuse from automated scripts and unauthorized endpoints.

To protect data at rest and in transit, firms must deploy End-to-End Encryption (E2EE) for messaging and transaction data, apply tokenization to sensitive fields (e.g., card numbers), and implement AES-256 encryption for databases. Regular key rotation and access audits should be mandatory.

Adopting a zero-trust security framework involves verifying all access requests regardless of location. Companies should enforce least-privilege access controls, use network segmentation, and implement identity verification for internal users to mitigate insider threats.

AI and Machine Learning models should be trained on large datasets of fraudulent patterns to detect anomalies in transaction behaviour. These systems should support adaptive learning to evolve with emerging fraud techniques and include automated response capabilities (e.g., transaction blocking, and alerts).

For regulators, concrete actions include mandating independent security audits, requiring compliance with global standards such as ISO/IEC 27001, PCI-DSS, and GDPR, and encouraging the use of regulatory sandboxes to test new security technologies. Regulators should also establish incident reporting frameworks and enforce timely disclosure of breaches to affected stakeholders.

By providing these specific technical and policy-based recommendations, the conclusion would more effectively guide both industry players and policymakers in addressing the systemic security risks facing the digital financial ecosystem.

References

[1] Shrier, D. et al., "Global Fintech," *The MIT Press eBooks*, 2022. [Online]. Available: https://doi.org/10.7551/mitpress/13673.001.0001

[2] Allen, F., Gu, X., and Jagtiani, J., "A Survey of Fintech Research and Policy Discussion," *Review of Corporate Finance*, vol. 1, no. 3–4, pp. 259–339, 2021. [Online]. Available: https://doi.org/10.1561/114.00000007

[3] Dwivedi, Y. K. et al., "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *International Journal of Information Management*, vol. 66, p. 102542, 2022. [Online].

Available: https://doi.org/10.1016/j.ijinfomgt.2022.102542
[4] Gill, I. S., Packard, T. G., and Yermo, J., "Keeping the promise of social security in Latin America," *The World Bank eBooks*, 2004. [Online]. Available: https://doi.org/10.1596/0-8213-5817-0
[5] Warner, K. S. and Wäger, M., "Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal," *Long Range Planning*, vol. 52, no. 3, pp. 326–349, 2018. [Online]. Available: https://doi.org/10.1016/j.lrp.2018.12.001
[6] Böhme, R., Christin, N., Edelman, B., and Moore, T., "Bitcoin: Economics, Technology, and Governance," *The Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015. [Online]. Available: https://doi.org/10.1257/jep.29.2.213
[7] Yaacoub, J. A. et al., "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems*, vol. 77, p. 103201, 2020. [Online]. Available: https://doi.org/10.1016/j.micpro.2020.103201
[8] Bagby, J. and Packin, N., "ReGTech and Predictive Lawmaking: Closing the RegLaG between prospective regulated activity and regulation," *Michigan Business & Entrepreneurial Law Review*, vol. 10, no. 2, p. 127, 2021. [Online]. Available: https://doi.org/10.36639/mbelr.10.2.regtech
[9] Beaman, C. et al., "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers & Security*, vol. 111, p. 102490, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102490
[10] Corbet, S., Lucey, B., Urquhart, A., and Yarovaya, L., "Cryptocurrencies as a financial asset: A systematic analysis," *International Review of Financial Analysis*, vol. 62, pp. 182–199, 2018. [Online]. Available: https://doi.org/10.1016/j.irfa.2018.09.003
[11] Treleaven, P. et al., "The future of cybercrime: AI and emerging technologies are creating a cybercrime tsunami," *SSRN Electronic Journal*, 2023. [Online]. Available: https://doi.org/10.2139/ssrn.4507244
[12] Daah, C., Qureshi, A., Awan, I., and Konur, S., "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," *Electronics*, vol. 13, no. 5, p. 865, 2024. [Online]. Available: https://doi.org/10.3390/electronics13050865
[13] Faotu, H., Asheshemi, O. N., and Jeremiah, E. T., "Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and AI-Driven Machine Learning Countermeasures," *Journal of Science and Technology*, vol. 30, no. 1, pp. 72–84, 2024. [Online]. Available: https://doi.org/10.20428/jst.v30i1.2597
[14] Yash, R., "Beyond the code: exploring the human factor in cybersecurity through social engineering," 2023.
[15] Solove, D. J., *The Digital Person: Technology and Privacy in the Information Age*, *Choice Reviews Online*, vol. 42, no. 09, p. 42–5512, 2005. [Online]. Available: https://doi.org/10.5860/choice.42-5512
[16] Hileman, G. and Rauchs, M., "2017 Global Blockchain Benchmarking Study," *SSRN Electronic Journal*, 2017. [Online]. Available: https://doi.org/10.2139/ssrn.3040224
[17] Tobias, A., "Cryptocurrencies and Decentralized Finance," *International Monetary Fund*, 2022. [Online]. Available: https://www.imf.org/en/News/Articles/2022/06/24/sp083022-crptocurrencies-and-decentralized-finance
[18] Eli, D., "Cryptocurrency," 2014. [Online]. Available: https://www.researchgate.net/publication/29872075_Cryptocurrency
[19] Wolfgang, K. H., Campbell, R. H., and Raphael, C. G., *Understanding Cryptocurrencies*, 2019.
[20] Conti, M., Kumar, E. S., Lal, C., and Ruj, S., "A survey on security and privacy issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018. [Online]. Available: https://doi.org/10.1109/comst.2018.2842460
[21] Anagnostopoulos, I., "Fintech and regtech: Impact on regulators and banks," *Journal of Economics and Business*, vol. 100, pp. 7–25, 2018. [Online]. Available: https://doi.org/10.1016/j.jeconbus.2018.07.003
[22] Wang, Y. et al., "A survey on metaverse: fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 319–352, 2022. [Online]. Available: https://doi.org/10.1109/comst.2022.3202047
[23] Rose, S., Borchert, O., Mitchell, S., and Connelly, S., "Zero Trust Architecture," *NIST Special Publication 800-207*, 2020. [Online]. Available: https://doi.org/10.6028/nist.sp.800-207
[24] Faotu, H. and Jeremiah, E. T., "AI and SaaS Embedded System: Enhancing Content Creation Through Contextual Language," *Journal of Science and Technology*, vol. 29, no. 2, pp. 57–66, 2024. [Online]. Available: https://doi.org/10.20428/jst.v29i2.2447
[25] Gill, S. S. et al., "AI for next generation computing: Emerging trends and future directions," *Internet of Things*, vol. 19, p. 100514, 2022. [Online]. Available: https://doi.org/10.1016/j.iot.2022.100514
[26] Zou, Y., Zhu, J., Wang, X., and Hanzo, L., "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016. [Online]. Available: https://doi.org/10.1109/jproc.2016.2558521