INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

The Future of Cybersecurity in Payment Systems: From Preventing Attacks to Building Trust in The Global Digital World

[1]Sule Magaji, [1]Yahaya Ismail, [2]Yakubu Jafaru, [1]Ibrahim Musa

[1]Department of Economics University of Abuja

[2]Department of Sociology, University of Abuja

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1407000074

Received: 06 July 2025; Accepted: 11 July 2025; Published: 11 August 2025

Abstract: This study investigates the evolving role of trust as a central pillar in contemporary cybersecurity strategies within global payment systems. Employing a qualitative meta-analytical approach and multi-case comparative analysis, the research explores how trust influences the design, adoption, and regulation of three major payment innovations: mobile money platforms in sub-Saharan Africa, cryptocurrency ecosystems, and central bank digital currencies (CBDCs) in Nigeria, China, and Sweden. Data were drawn from empirical studies and institutional reports, analysed using thematic content analysis. The findings reveal that technical security alone is insufficient for user engagement; instead, institutional credibility, regulatory assurance, and positive user experience significantly drive trust. In low-resource settings, such as Africa, platforms like M-Pesa gain user confidence through reliability and accessibility. In contrast, in cryptocurrency markets, systemic failures like FTX erode trust despite blockchain transparency. For CBDCs, adoption depends largely on public confidence in state institutions and their data protection practices. The study concludes that the future of cybersecurity must shift from reactive threat mitigation to proactive trust-building, emphasising trust-by-design, digital literacy, regulatory transparency, and international cyber norms. Trust is not a secondary outcome of secure systems—it is the strategic foundation upon which they must be built.

Keywords: Trust in cybersecurity; payment systems; mobile money; cryptocurrency; digital finance; financial technology Introduction.

I. Introduction

The financial world is undergoing a profound transformation driven by rapid advances in digital technology (Magaji, Darma, & Igwe, 2021). Digital payment systems, encompassing mobile banking applications, e-wallets, contactless cards, blockchain-based transactions, real-time settlement systems, and central bank digital currencies (CBDCs), have emerged as key enablers of commerce and financial inclusion in the 21st century (Magaji, Musa, & Dogo, 2023). These technologies are not only reshaping how individuals, businesses, and governments transact but also redefining the very infrastructure of the global financial system (Magaji, Musa, Ahmad & Eke, 2024). From urban centers in developed economies to rural communities in emerging markets, digital payment platforms have facilitated unprecedented access to financial services, reducing reliance on cash and traditional banking (Musa & Magaji, 2024; World Bank, 2022).

However, alongside these benefits come profound vulnerabilities. As digital payments become increasingly ubiquitous, they are attracting the attention of cybercriminals, hacktivists, and state-sponsored actors (Magaji, Ismail & Musa, 2025). High-profile breaches of payment processors, ransomware attacks on financial institutions, and data leaks from fintech platforms have exposed systemic weaknesses (IBM Security, 2023). These incidents not only result in financial losses but also erode public confidence in digital platforms. As cyber threats grow in scale and sophistication, a purely defensive or reactive approach to cybersecurity is proving inadequate (Magaji & Musa, 2023). The traditional emphasis on preventing attacks through technical measures, such as firewalls, encryption, and intrusion detection systems, while still essential, is no longer sufficient on its own (Anderson, 2020).

This article argues that the primary cybersecurity challenge for the future of payment systems is not merely to prevent every potential intrusion, but to build and maintain trust in a global, digitised financial environment. Trust must become the organising principle around which cybersecurity efforts are structured (Magaji & Yisa, 2023). Without it, even the most technologically advanced systems will struggle to adopt and utilise effectively. Trust, in this context, encompasses more than system integrity; it also includes the belief that one's data will be handled ethically, that transactions will be processed reliably, and that privacy and accountability will be maintained even in the face of inevitable breaches (OECD, 2021).

Importantly, trust is not a static attribute; it is dynamic and earned continuously. It depends on how organisations respond to cyber incidents, how transparently they communicate risks, how consistently they uphold ethical standards, and how inclusive their platforms are for all segments of society. In a hyperconnected global economy where users frequently interact with digital financial services across borders, currencies, and diverse regulatory environments, building trust presents both technical and socio-political challenges (Eke, Osi, Sule & Musa, 2023). Stakeholders, including banks and fintech companies, regulators, and consumers, must collaborate to create payment systems that are not only secure by design but also transparent, user-centric, and governed by shared principles of accountability (Gabdo & Sule, 2023; World Economic Forum, 2023).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

As this paper will demonstrate, the future of cybersecurity in payment systems lies in shifting from a narrow, adversarial view of cybersecurity (focusing on threats and defences) toward a holistic, trust-driven framework. Such a shift involves integrating privacy by design, adopting transparent AI systems for fraud detection, enforcing global regulatory standards, and fostering a culture of digital literacy (NIST, 2022). In doing so, payment systems can sustain the confidence of users and institutions, even in an environment where cyber threats are persistent and constantly evolving (Magaji & Yahaya, 2012).

While securing digital payment systems against malicious actors remains a critical priority, trust the collective perception of safety, fairness, and responsibility will ultimately determine the resilience and longevity of these systems in the digital age. The remainder of this article examines the contours of this trust-centred approach and its implications for the future of cybersecurity in the global financial landscape.

II. Literature Review

The Evolution of Cybersecurity in Payment Systems: Traditionally, cybersecurity in payment systems has centred on technical fortifications, firewalls, intrusion detection systems, anti-malware tools, and encryption protocols. These solutions focused on perimeter defence, aiming to keep attackers out. However, recent breaches (e.g., SWIFT hacks, fintech platform breaches, and ransomware attacks on payment processors) demonstrate that no system is immune. Cybersecurity is evolving beyond securing systems to fostering confidence among users, especially in an environment where threats are persistent and sophisticated.

The Crisis of Trust in the Digital Economy: Trust deficits are emerging as a critical weakness in payment systems. Consumers hesitate to use new digital platforms if they fear data theft, identity fraud, or financial loss (Ismail, El-Yaqub & Eke, 2025). Institutions struggle to navigate a fragmented regulatory environment where accountability and enforcement are inconsistent, and youth unemployment is prevalent (Magaji, Musa, & Salisu, 2022). Moreover, the proliferation of deepfakes, AI-powered phishing, and synthetic identity fraud further undermines confidence. Building trust is no longer a passive outcome of robust systems, but an active and strategic objective of cybersecurity frameworks.

Trust as the New Cybersecurity Paradigm: Trust-building involves transparent communication, user education, the integration of ethical AI, and effective redress mechanisms. Technologies such as blockchain enable immutable transaction records, improving auditability. Multi-factor authentication (MFA), zero-trust architecture, and real-time anomaly detection enhance both security and user assurance.

Human-Centric Design: Cybersecurity Must Prioritise User Experience. Systems that are too complex can lead to poor password practices or the development of workarounds. Payment platforms should be designed to empower users with clear information, privacy controls, and responsive support. Psychological security—the sense that systems are fair and comprehensible—is integral to digital trust.

Regulatory and Ethical Foundations: Globally harmonised regulations, such as the EU's GDPR and PSD2, as well as emerging AI acts, establish baseline protections. Similarly, payment security standards (e.g., PCI DSS) and frameworks such as ISO/IEC 27001 contribute to institutional trust. The ethical use of data, cross-border cooperation, and consistent enforcement are essential.

Artificial Intelligence and Machine Learning: AI plays a dual role, enhancing fraud detection and real-time response, while also being leveraged by attackers. Trustworthy AI must be explainable, fair, and aligned with regulatory standards. Adaptive AI systems that learn from transaction behaviours improve security while preserving usability.

Blockchain and Distributed Ledger Technologies: Decentralised platforms increase transparency and reduce single points of failure. Smart contracts in payment systems ensure the automatic execution of transactions based on predefined rules, thereby reducing human error and the potential for fraud. However, governance and interoperability issues remain barriers.

Quantum-Resistant Security: As quantum computing poses a threat to current cryptographic algorithms, transitioning to quantum-resistant methods is crucial. This future-proofing reinforces long-term trust in the confidentiality and integrity of payment systems.

Theoretical Framework

This study is anchored on three interrelated theoretical foundations: Sociotechnical Systems Theory, Trust Theory, and the Technology Acceptance Model (TAM). Together, these theories provide a multidimensional lens for analyzing how digital payment systems are shaped not only by technological defenses but also by social perceptions, institutional credibility, and user behavior factors that are critical to building and sustaining trust.

Sociotechnical Systems Theory posits that effective system design and performance require a harmonious integration of both technical subsystems (hardware, software, cybersecurity protocols) and social subsystems (people, institutions, cultures, norms) (Trist & Emery, 1973). In the context of digital payment platforms, cybersecurity cannot be isolated from user experience, organisational practices, or regulatory governance.

This theory is central to understanding why technical security measures such as firewalls or cryptographic algorithms, while essential, are insufficient if users lack trust in the institutions behind them. For example, a technically secure central bank digital currency (CBDC) may fail in adoption if people fear government surveillance. Likewise, decentralised blockchain systems may

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

offer transparency but still struggle with public trust due to high-profile fraud cases or media scepticism. Thus, the sociotechnical perspective reinforces the idea that cybersecurity is as much a human challenge as it is a technical one.

Trust Theory: Trust Theory provides a behavioural and psychological framework for analysing how users interact with digital systems. According to Mayer, Davis, and Schoorman (1995), trust is a function of **ability, integrity, and benevolence**—that is, the belief that a system or institution is competent, honest, and has the user's interests at heart.

In digital payment systems, trust must be cultivated at multiple levels:

Interpersonal trust, where users interact with mobile money agents or customer service representatives;

Institutional trust, based on perceptions of regulatory protection and ethical data handling;

Technological trust, where users believe in the reliability, security, and privacy of the platform itself.

These dimensions help explain adoption patterns, resistance to new systems, or panic in response to cyber incidents. Trust Theory thus provides a conceptual bridge between user behaviour and system design, validating the article's thesis that trust, not merely technical deterrence, is the future of cybersecurity in financial systems.

Technology Acceptance Model (TAM): The Technology Acceptance Model (Davis, 1989) explains how users come to accept and use a new technology. It identifies two primary determinants:

Perceived usefulness – the degree to which a user believes the technology enhances their transaction experience;

Perceived ease of use – the degree to which the system is free of effort or complexity.

In cybersecurity discourse, TAM emphasises that, regardless of a payment system's security, it must also be usable, intuitive, and convenient to encourage adoption. Complex authentication procedures or poorly designed user interfaces can lead users to abandon secure platforms in favour of less secure, but easier-to-use, alternatives.

Moreover, trust acts as a mediating factor in TAM. Recent extensions of the model, such as the Technology Acceptance Model 2 (TAM2) and the Unified Theory of Acceptance and Use of Technology (UTAUT), incorporate social influence and trust as key factors in technology adoption (Venkatesh & Davis, 2000). Therefore, the role of trust in shaping both perceived usefulness and ease of use further justifies its centrality in cybersecurity policy for digital finance.

By synthesizing these three theories, the study constructs a holistic framework that captures the technical, behavioral, and systemic dynamics of cybersecurity in digital payment ecosystems. While Sociotechnical Systems Theory frames the interconnectedness of security design and social systems, Trust Theory deepens our understanding of user psychology and institutional confidence. Meanwhile, the Technology Acceptance Model contextualises the usability dimension of secure platforms and how it intersects with trust-based adoption behaviour.

This theoretical foundation justifies the article's central argument: the long-term effectiveness of cybersecurity in payment systems will be determined not just by attack prevention, but by the trustworthiness, transparency, and usability of the systems themselves.

Empirical Review

Abdulazeez and Magaji (2023) explore the foundational elements of Nigeria's electronic banking cyberinfrastructure. They emphasised that this system was established to enhance the convenience of banking, reduce physical cash usage, and potentially lower crime rates, such as armed robbery and corruption. The chapter aims to investigate how effectively this digital system has reduced or transformed the nature of criminal activities. It utilises police crime statistics, interviews with security personnel, and social surveys to compare criminal patterns before and after the implementation of cyberbanking security systems. Analysis was carried out using simple percentages, frequency distributions, and Likert scale responses. Findings highlight a notable disparity in electronic banking-related crimes, particularly a rise in kidnapping, between Kaduna and Abuja. The study recommends regular maintenance and rigorous testing of banking hardware and software to ensure security and prevent loss of depositor funds.

Magaji, Hassan, and Temitope (2022) investigate the relationship between electronic banking and the rise in criminal activities, focusing on Kaduna metropolis. The study employed a systematic sampling technique, using Taro Yamane's formula to determine the sample size, and collected data from 400 residents through semi-structured questionnaires, interviews, and audio recordings. Data analysis involved percentage methods, frequency tables, and logit regression. Results indicated that while the overall crime rate declined in frequency and occurrence, new forms of crime, particularly ATM-related theft and kidnapping for ransom, emerged. The study concluded that the Central Bank of Nigeria, in collaboration with commercial banks, must adopt urgent measures leveraging ICT tools to manage the evolving crime patterns brought about by the adoption of electronic banking in Nigeria.

Abdulazeez, Magaji, and Musa (2022) examine infrastructure-related obstacles that have hindered the success of the cashless policy introduced by the Central Bank of Nigeria in 2012, using data from Kaduna State. Data were collected through structured questionnaires and interviews with various stakeholders, including bank customers, officials, and security operatives. Using simple percentages and frequency distributions for analysis, the study identified recurring problems, including network breakdowns, ATM failures that prevented cash dispensation after account debits, and slow bank responses to transaction issues. These issues have led

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

to cyber fraud and a decline in public trust in the banking system. The researchers recommend that banks implement mandatory infrastructure improvements and that both banks and regulatory bodies adopt stronger cybersecurity measures.

Ibukuoluwa, Magaji, and Musa (2025) evaluate the impact of digital financial services on the distribution of humanitarian aid in Lagos State, specifically examining the role of financial technology in enhancing efficiency and reducing resource leakage. A quantitative approach with stratified random sampling was used to collect data from 400 participants in Lagos Island, Alimosho, Mushin, and Ikorodu LGAs. Multiple regression was employed to analyse relationships between humanitarian aid effectiveness and variables such as financial inclusion, adoption of digital services, policy environment, and socio-economic status. The results showed a weak but positive correlation between digital service adoption and effective aid distribution, with challenges such as poor network connectivity and high transaction costs hindering success. The study recommends strengthening regulatory policies, improving service reliability, and introducing targeted financial education to maximise the benefits of fintech in humanitarian efforts.

Magaji and Ahmad (2024) examine the impact of non-performing loans (NPLs) on the operations of Deposit Money Banks (DMBs) in Nigeria within the context of digital banking. Data from eight selected banks, provided by the Central Bank of Nigeria, were analysed using the Panel ARDL model. Return on equity (ROE) was the metric for assessing performance. The findings indicated that NPLs have a negative correlation with bank performance, although the overall impact was not substantial after digitalisation. The regression coefficient of -1.234659 confirmed an inverse relationship between NPLs and ROE. This research contributes to the understanding of how digitalization can mitigate the adverse effects of loan defaults, suggesting that continued digital banking reforms could support improved performance among Nigerian banks.

Alalwan et al. (2018) found that perceived security and trust were the most significant predictors of user willingness to adopt mobile financial services in the Middle East. Their research demonstrated that even when robust encryption and authentication mechanisms were in place, users remained hesitant if they did not perceive the service provider as trustworthy. Similarly, Oliveira et al. (2017) employed structural equation modelling to assess the adoption of mobile payment platforms in Europe. They concluded that trust in the system, trust in the provider, and past experiences directly influenced behavioural intentions more than purely technical safeguards.

In sub-Saharan Africa, empirical work by GSMA (2021) on mobile money usage across 15 countries found that agent network reliability and user education were crucial for developing trust. The study revealed that users were more likely to repeatedly use mobile payment platforms when they had direct and consistent interactions with knowledgeable and trustworthy agents, suggesting that human intermediaries still play a vital role in shaping perceptions of digital safety.

Cryptocurrency adoption presents a different dynamic. A global survey by PwC (2022) found that over 60% of respondents who refrained from investing in or using cryptocurrencies cited "lack of trust in platforms and regulation" as the main deterrent. Similarly, a cross-country study by Auer et al. (2022) on CBDC trials found that public trust in central banks and government transparency were significant factors in determining user engagement with state-issued digital currencies. Their findings from pilot programs in Sweden, the Bahamas, and Nigeria emphasise that public fears over surveillance and data misuse could substantially limit CBDC uptake regardless of technical readiness.

These empirical insights affirm the central thesis of this article: that cybersecurity strategies in payment systems must be reframed around trust creation and preservation, rather than solely focusing on attack mitigation. They also suggest a multidimensional framework for trust that includes institutional reputation, technical transparency, regulatory clarity, and user empowerment.

III. Methodology

This article employs a qualitative meta-analytical approach combined with case study analysis to evaluate how trust has emerged as the focal point in contemporary cybersecurity strategies within global payment systems. The methodology integrates scholarly literature, empirical studies, regulatory reports, and institutional assessments to build a synthesised understanding of the evolving cybersecurity paradigm.

Research Design: The research follows a multi-case, comparative analysis design. Three core case areas were selected: mobile payments in sub-Saharan Africa (focusing on M-Pesa and MTN Mobile Money), cryptocurrency ecosystems (including Bitcoin, Ethereum, and exchanges such as Binance and FTX), and central bank digital currencies (CBDCs) currently under pilot in Nigeria, China, and Sweden. These cases were purposefully selected to represent diverse technological, geographic, and institutional contexts. The primary objective was to identify common trust-related themes that spanned these systems.

Data Collection: Data were collected through secondary sources, including peer-reviewed journals (e.g., *American Economic Review, Science*), institutional white papers (e.g., IMF, World Bank, BIS), and authoritative industry reports (e.g., GSMA Mobile Money Reports, IBM Cost of Data Breach). The inclusion criteria for these sources were: (a) publication within the last 10 years, (b) explicit analysis of trust or security in payment systems, and (c) use of quantitative or qualitative methods.

To ensure comprehensiveness, reports and surveys from regulatory bodies, such as the OECD, the European Central Bank (ECB), the SEC, and national central banks, were also included. A total of 43 empirical documents and 15 policy and technical reports were reviewed.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Data Analysis: The data analysis employed thematic content analysis, categorising findings based on four dimensions of trust: technical reliability, institutional credibility, user perception, and regulatory assurance. Cross-case synthesis was used to identify patterns and divergences in trust dynamics across regions and technologies.

Limitations: One limitation of this study is its reliance on secondary data, which may not fully capture evolving sentiments in real-time payment environments. Furthermore, given the dynamic nature of digital finance, some data may quickly become outdated. Nonetheless, the triangulation of diverse and credible sources helps mitigate these limitations and provides a robust foundation for the paper's conclusions.

IV. Results

Case Studies and Global Trends: The need to shift cybersecurity from mere attack prevention to fostering trust is becoming increasingly evident in the evolution of different regions and technologies. Examining real-world implementations of digital payment systems reveals a complex interplay between innovation, regulation, and public confidence. This section presents three illustrative cases of mobile payments in Africa, cryptocurrency ecosystems, and central bank digital currencies (CBDCs), each offering unique insights into the role of trust in the future of cybersecurity.

Mobile Payments in Africa: Africa has become a global leader in mobile money innovation, not due to technological superiority, but due to necessity and creativity. The continent's limited access to traditional banking infrastructure spurred the development of alternative financial tools, with Kenya's M-Pesa being the most iconic example. Launched in 2007 by Safaricom and Vodafone, M-Pesa enabled users to deposit, withdraw, transfer money, and pay for goods and services through basic mobile phones—no internet required (Jack & Suri, 2014).

What makes mobile payments in Africa particularly compelling is the level of trust they have engendered among populations historically excluded from formal banking. Despite lacking advanced digital literacy, users adopted platforms like M-Pesa, MTN Mobile Money, and Airtel Money because of their consistent reliability, robust agent networks, and perceived transparency. Studies show that the use of mobile money has led to increased household savings and financial resilience in rural areas (Suri & Jack, 2016).

The trust in these systems has been built through a combination of factors, including simple user interfaces, strong regulatory oversight in certain regions, and a feedback loop of positive user experiences. For instance, real-time confirmations of transactions provide psychological assurance, while the visibility of mobile money agents in every village fosters a sense of accessibility and accountability (GSMA, 2021). However, mobile money services are not without challenges. Fraud, SIM-swap scams, and lack of interoperability between platforms can erode trust if not addressed promptly. The future of mobile payments in Africa will depend on further strengthening cybersecurity frameworks and user education without compromising the simplicity that made these services successful (Manbe, Magaji & Damagun, 2014).

Cryptocurrency Ecosystems: Cryptocurrencies such as Bitcoin, Ethereum, and newer decentralised finance (DeFi) tokens have transformed the payment landscape by offering a radical alternative to government-backed currencies. Built on blockchain technology, cryptocurrencies promise decentralisation, immutability, and transparency—qualities that, in theory, should engender trust (Nakamoto, 2008). However, in practice, trust in cryptocurrency ecosystems is complex and often fragile.

Unlike traditional banking systems, where institutions and regulators provide safety nets, cryptocurrencies rely on the code and community for security and governance. While the transparency of blockchain ledgers allows anyone to verify transactions, this openness does not inherently protect users from fraud, phishing attacks, or the collapse of exchanges, as evidenced by the 2022 failure of FTX, a significant cryptocurrency exchange, which resulted in billions of dollars in investor losses (SEC, 2023). These events damage public trust and fuel regulatory crackdowns globally.

Moreover, the volatile nature of crypto assets, compounded by speculative trading and misinformation, makes users sceptical about adopting them for everyday transactions. Regulatory uncertainty also contributes to distrust, as countries differ significantly in their approach to cryptocurrencies, ranging from outright bans to full acceptance. For instance, while El Salvador adopted Bitcoin as legal tender, other nations, such as China, have banned crypto-related activities, citing concerns over financial instability and security (OECD, 2022).

To establish lasting trust in cryptocurrency payment systems, developers and institutions must prioritise user protection, transparency in governance, and compliance with global financial standards (Eke, Magaji & Osi, 2022). The emergence of regulatory frameworks, such as the European Union's MiCA (Markets in Crypto-Assets) legislation, and an increased emphasis on Know Your Customer (KYC) protocols signal a movement toward trust-driven crypto regulation. Without such measures, the promise of decentralisation may be overshadowed by the risks of manipulation, fraud, and misuse.

Central Bank Digital Currencies (CBDCs) and Institutional Trust: A rapidly growing trend in digital finance is the development of Central Bank Digital Currencies (CBDCs) (Abdullahi, Magaji & Musa, 2024). These are digital representations of national currencies, issued and backed by central banks, designed to enhance financial inclusion, reduce reliance on physical cash, counter the influence of private cryptocurrencies (BIS, 2021), and promote smooth monetary policy implementation (Magaji, Ayo, Ibrahim & Ali, 2019). More than 130 countries, including China, Nigeria, Sweden, and the United States, are exploring or piloting CBDCs (Atlantic Council, 2024).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

The success of CBDCs, however, hinges on public trust in institutional intent and technical security. Unlike cryptocurrencies, CBDCs are centralised and subject to state control, raising concerns about privacy, surveillance, and potential government overreach. In nations with a history of weak institutions or political repression, the public may be wary of using state-issued digital currencies due to concerns about being monitored or restricted. Conversely, in well-regulated environments, CBDCs can offer faster payments, lower transaction costs, and greater stability compared to private payment platforms.

For example, Nigeria launched the eNaira in 2021 as Africa's first CBDC, aiming to improve financial access and reduce transaction costs. However, adoption has been slow due to limited user awareness and scepticism about data privacy (IMF, 2023). Similarly, China's Digital Yuan has undergone extensive trials, but its long-term adoption will depend on how the state addresses privacy concerns and ensures fair usage without coercion.

To build trust in CBDCs, central banks must engage in transparent policymaking, adopt privacy-by-design principles, and communicate clearly about how data is collected and protected. Public education, pilot programs with private stakeholders, and international interoperability standards will be key in ensuring that CBDCs are seen not as instruments of control but as tools of empowerment and economic resilience.

V. Findings

This study examines the evolving role of trust as a central pillar of cybersecurity in the digital payment ecosystem. Drawing from a multi-case comparative analysis, empirical literature, and theoretical insights, the following key findings emerged:

Trust is Foundational to Cybersecurity Effectiveness: Across all three case domains—mobile payments in Africa, cryptocurrency ecosystems, and central bank digital currencies (CBDCs)—trust consistently emerged as a determinant of system success or failure. Users were more inclined to adopt and continue using payment platforms not solely because of technical security, but because of their confidence in the system's reliability, fairness, transparency, and ethical governance.

Technical Security Is Necessary but Not Sufficient: The study confirms that while cybersecurity technologies (e.g., encryption, authentication, and blockchain) are critical, they alone do not guarantee user engagement or systemic resilience. For example, although cryptocurrencies utilise highly secure blockchain protocols, trust in the broader crypto ecosystem remains low due to exchange failures, regulatory ambiguity, and perceived risks of fraud.

Institutional Credibility and Regulatory Assurance Drive User Trust: Public confidence in institutions—whether private payment platforms, crypto exchanges, or central banks—greatly influences user trust. In the case of CBDCs, for instance, adoption levels were directly tied to citizens' perceptions of government intentions, transparency, and privacy safeguards. Weak regulatory environments or opaque policies diminished trust regardless of the system's technical sophistication.

User Experience and Digital Literacy Shape Perceptions of Security: The usability and accessibility of payment systems influence not only convenience but also perceived safety. Mobile money platforms, such as M-Pesa, have succeeded in low-resource settings by combining technical reliability with user-friendly interfaces and accessible customer support. In contrast, overly complex or poorly explained systems can cause users to disengage or migrate to less secure alternatives.

Global Trends Reflect a Shift Toward Trust-Centric Cybersecurity Models: A growing consensus is emerging among policymakers and industry leaders that cybersecurity in financial systems must evolve from reactive threat mitigation to proactive trust-building. Frameworks emphasising trust-by-design, data privacy, public-private collaboration, and regulatory transparency are gaining momentum globally, as seen in the EU's MiCA regulation and various CBDC pilot programs.

The study finds that the future of cybersecurity in payment systems will hinge not just on fending off cyber threats, but on the ability of systems and institutions to foster sustained, multi-level trust. This trust must encompass the technology itself, the entities behind it, and the regulatory environments in which they operate.

Policy and Strategy Recommendations

1. Adopt Trust-by-Design Principles: Security should be embedded from the ground up with user-centric principles.
2. Strengthen Public-Private Partnerships: Collaboration among governments, tech companies, and financial institutions fosters a resilient cybersecurity ecosystem.
3. Invest in Cyber Hygiene and Literacy: Widespread digital literacy and cybersecurity awareness are essential to prevent social engineering attacks.
4. Enhance Transparency and Accountability: Real-time reporting of breaches, independent audits, and user compensation schemes enhances public trust.
5. Establish International Cyber Norms: Multilateral agreements on digital trust, cybercrime prosecution, and payment interoperability are necessary in a borderless digital economy.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

VI. Conclusion

The future of cybersecurity in payment systems is not confined to stopping attacks; it is about building, maintaining, and restoring trust. In an age where digital transactions underpin daily life and economic growth, secure systems that are perceived as opaque or fragile will fail to inspire user confidence. The next generation of cybersecurity must be proactive, inclusive, ethical, and deeply integrated into the human and regulatory fabric of global finance. Trust is not merely a byproduct of security; it is its very purpose.

References

1. Abdulazeez, H., & Magaji, S. (2023). Nexus between Banking Cybersecurity Breaches, Cyber Vulnerabilities, and Kidnap for Ransom in Nigeria: A Comparative Analysis of Kaduna and Abuja Metropolis, Nigeria. In Cybersecurity for Decision Makers (pp. 279–292). CRC Press.
2. Abdulazeez, H., Magaji, S., & Musa, I. (2022). Analysis of Infrastructural Challenges, Cybercrime, and the Cashless Policy in Nigeria: Infrastructural Challenges, Cybercrime, and the Cashless Policy ", ARIS2-Journal, vol. 2, no. 1, pp. 13–27, Aug. 2022.
3. Abdullahi, A. I., Magaji, S. & Musa, I. (2024). Navigating technological shifts: The role of Digital Strategies in Modern Banking. International Journal of Novel Research in Marketing Management and Economics, 11(2), 13-28
4. Alalwan, A. A., Dwivedi, Y. K., & Williams, M. D. (2018). Consumer adoption of mobile payment services: An empirical study. Journal of Retailing and Consumer Services, 45, 168–182. https://doi.org/10.1016/j.jretconser.2018.08.005
5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
6. Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.
7. Atlantic Council. (2024). Central bank digital currency tracker. https://www.atlanticcouncil.org/cbdctracker/
8. Auer, R., Cornelli, G., & Frost, J. (2022). Rise of Central Bank Digital Currencies: Drivers, Approaches, and Technologies. BIS Working Papers.
9. Bank for International Settlements (BIS). (2021). CBDCs: Financial stability implications. https://www.bis.org/publ/othp42.pdf
10. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
11. Eke, C. I., Magaji, S. & Osi, U.M. (2022). Technical Assessment of Financial Technologies in Nigeria. Probability Statistics and Econometric Journal 4 (5), 1-15
12. Eke, C. I., Osi, U.M., Sule, M. & Musa, I. (2023). State Control of Digital-Fiat-Electronic Currency Transmission in an Economy: The Case for a Hybrid Currency. Asian Journal of Economics, Finance and Management, 92-96
13. European Central Bank. (2022). Central Bank Digital Currencies: Building Trust in a Digital Era.
14. Gabdo, A. L., & Sule, M. (2023). Examining the Relationship Between Urban Sustainable Development and Quality Education in FCT Abuja, Nigeria. African Journal of Environment and Sustainable Development| ISSN 3027, 2718.
15. GSMA. (2021). State of the Industry Report on Mobile Money 2021. https://www.gsma.com/mobilemoney/
16. GSMA. (2021). State of the Industry Report on Mobile Money. https://www.gsma.com/mobilemoney
17. IBM Security. (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach
18. Ibukuoluwa, N. D., Magaji, S., & Musa, I. (2025). The Impact of Digital Financial Services on Nigeria's Distribution of Humanitarian Aid. International Journal of Social Science Exceptional Research 4(3), 50-59.
19. International Monetary Fund (IMF). (2023). The eNaira and Nigeria's Digital Financial Inclusion. https://www.imf.org/
20. Ismail, Y., El-Yaqub, A.B. & Eke, C. I., (2025) Impact of Digital Payment Technologies on Selected Banking Institutions in Nigeria. MSI Journal of Economics and Business Management. 2(4), 1-10. DOI: 10.5281/zenodo.15173057
21. Jack, W., & Suri, T. (2014). Risk Sharing and Transaction Costs: Evidence from Kenya's Mobile Money Revolution. American Economic Review, 104(1), 183–223. https://doi.org/10.1257/aer.104.1.183
22. Magaji, S., & Ahmad, A. I. (2024). Assessment of Non-Performing Loans on Deposit Money Banks' Performance During the Digital Banking Policy in Nigeria. International Journal of Research Publication and Reviews, Vol 5, no 4, pp 9625-9634
23. Magaji, S., & Musa, I. (2023). Analysis of the impact of banking sector credit on the real sector. Asian Journal of Economics and Empirical Research, 10(1), 11–19.
24. Magaji, S., & Yisa, S. (2023). The Impact Of Agricultural Loans by Deposit Money Banks on Agricultural Output In Nigeria. International Journal of Indonesian Business Review, 2(2), 194–204.
25. Magaji, S., Ayo, A.A., Ibrahim, M. & Ali, S. (2019). Relative impact of monetary policy instruments on economic growth in Nigeria. Lapai Journal of Economics 3 (2), 93-118
26. Magaji, S., Darma, N.A. & Igwe, G.U. (2021). Testing the Supply-leading and Demand-following Hypothesis for Financial Development and Economic Growth–A Case of the Nigerian Banking System. GSJ 9 (12)
27. Magaji, S., Hassan, A., & Temitope, Y. A. (2022). Nexus between E-Banking and the Upsurge of Crime in Kaduna State, Nigeria. Lapai Journal of Economics, 6(1), 42–50.
28. Magaji, S., Ismail, Y. & Musa, I., (2025) Impact of institutional Quality on Human Capital Development in Nigeria. MSI Journal of Economics and Business Management. 2(2), 21-26. DOI:-10.5281/zenodo.14936039

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

29. Magaji, S., Musa, I. & Salisu, A. (2022). Impact of Insecurity on Youth Unemployment in Nigeria: O L S Estimation Technique (OLS). Indiana Journal of Economics and Business Management 2 (1), 4-9
30. Magaji, S., Musa, I., & Dogo, S. S. (2023). Analysis of the Impact of Banking Sector Credits on the Real Sector in Nigeria. International Journal of Management and Business Applied, 2(1), 12–20.
31. Magaji, S., Musa, I., Ahmad, A.I. & Eke, C.I. (2024). Linking Demonetisation to Small and Medium Enterprises (SMEs) Output. ijrpr 5 (3), 7487-7496
32. Magaji, S., Yahaya, H. (2012). Portrait of low savings in Africa. African Union Congress of African Economists. Available at: pages. au. int/.../Magaji_S PORTRAITOF_LOW_SAVINGS_IN_AFRI
33. Manbe, D. A., Magaji, S. & Damagun, Y.M. (2014). Cybercrimes and victimization: An analysis of economic cost implications for Nigeria. Proceedings Book of ICETSR 2014, Malaysia
34. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organisational trust. Academy of Management Review, 20(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335
35. Musa, I., & Magaji, S. (2024). Impact of Commercial Bank's Credit on Manufacturing Sector Output in Nigeria. Journal of Applied Economics in Developing Countries, 9(1), 1–9.
36. Musa, I., Magaji, S., & Elyaqub, A. B. (2023). Impact of Currency Redesign on Nigeria's Small and Medium-Sized Enterprises. Journal of Arid Zone Economy, 2(1), 74–84.
37. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
38. National Institute of Standards and Technology (NIST). (2022). Zero Trust Architecture (Special Publication 800-207).
39. National Institute of Standards and Technology (NIST). (2022). Zero trust architecture (Special Publication 800-207). https://doi.org/10.6028/NIST.SP.800-207
40. OECD. (2021). Digital Security Risk Management for Economic and Social Prosperity.
41. OECD. (2022). Regulatory approaches to crypto-assets. https://www.oecd.org/
42. Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2017). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Computers in Human Behaviour, 61, 404–414. https://doi.org/10.1016/j.chb.2016.03.030
43. Organisation for Economic Co-operation and Development (OECD). (2021). Digital security risk management for economic and social prosperity. https://www.oecd.org/sti/ieconomy/digital-security.htm
44. Payment Card Industry Security Standards Council (PCI SSC). (2024). Data Security Standards (DSS) v4.0.
45. Ponemon Institute. (2023). Cost of a Data Breach Report. IBM Security.
46. PwC. (2022). Global Crypto User Survey. **https://www.pwc.com/gx/en/industries/financial-services/assets/global-crypto-survey.pdf**
47. SEC. (2023). FTX and the Failure of Crypto Oversight. https://www.sec.gov/
48. Suri, T., & Jack, W. (2016). The Long-Run Poverty and Gender Impacts of Mobile Money: A Review of the Literature Science, 354(6317), 1288–1292. https://doi.org/10.1126/science.aah5309
49. Trist, E. L., & Emery, F. E. (1973). Towards a social ecology: Contextual appreciation of the future in the present. Plenum Press.
50. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926
51. World Bank. (2022). Digital financial services: Challenges and opportunities for emerging markets. https://www.worldbank.org/en/topic/financialinclusion/publication/digital-financial-services
52. World Economic Forum. (2023). Global cybersecurity outlook 2023. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/
53. World Economic Forum. (2023). Global Cybersecurity Outlook.