Delta Journal of Computing, Communications & Media Technologies (DJCCMT)
Journal platform–https://focjournals.dsust.edu.ng

Digital Economy Security Landscape: Challenges and Solutions

Duke Oghorodi
Department of Computer Science
Southern Delta University, Ozoro, Nigeria

Godwin Osakwe
Department of Cyber Security
Southern Delta University, Ozoro, Nigeria

Daniel Ukpenusiowho
Department of Software Engineering
Southern Delta University, Ozoro, Nigeria

Uwadia Francis*
Department of Cyber Security
Southern Delta University, Ozoro, Nigeria
John Ogbiti
Department of Computer Science
Edo State University, Iyamho, Nigeria

Paschal Chukwuemeka Nwankwo
Department of Information Technology, Nigerian British University, Asa, Nigeria

Wilson Nwankwo
Faculty of Computing
Southern Delta University, Ozoro, Nigeria.

ARTICLE INFO

Article history:
Received August 2024
Received in revised form Dec. 2024
Accepted December 2024
Available online Jan 2025

Keywords:
Digital Economy
Circular Economy
Cyber Infrastructure
Economy
Digital Divide

ABSTRACT

Digital technologies promise unprecedented economic growth, but they also introduce a complex security landscape that threatens inclusive development, particularly in countries facing significant infrastructural and socioeconomic disparities. This paper presents a narrative analysis of Nigeria's digital economy security environment, focusing on four interrelated challenge domains: (1) a persistent digital divide that limits equitable access to online services across urban and rural areas; (2) uneven digital literacy levels that impede citizens' safe and effective engagement with digital platforms; (3) a fragmented regulatory framework creating loopholes and inconsistent enforcement that stifle innovation; and (4) escalating cybersecurity threats—including data breaches, fraud, and malware—that erode public trust in digital transactions. To address these obstacles, we propose an integrated roadmap comprising: targeted infrastructure investments and public–private partnerships to expand broadband coverage; comprehensive digital education programs to develop cyber-savvy communities; establishment of a unified regulatory body to streamline policies and foster a secure innovation ecosystem; and deployment of advanced cybersecurity measures—including real-time threat monitoring, incident response protocols, and mandatory security standards—to protect critical digital assets. By implementing this multi-pronged approach,

Nigeria can bridge its digital divide, bolster its cyber defences, and emerge as a regional leader in the digital economy, driving sustainable, equitable, and inclusive economic growth.

Uwadia Francis

*Corresponding author.
E-mail address: uwadiaf@dsust.edu.ng

https://doi.org/10.xxx.
DJCCMT112025013

1. Introduction

The digital economy—encompassing all economic and social activities enabled by digital technologies and the internet—has emerged as a cornerstone of global growth, driving diversification, productivity gains, and novel business models (Alola et al., 2023; Amanullah et al., 2020). Its roots trace back to mainframe networks and ARPANET in the 1960s, evolving through the microprocessor and personal computer revolutions of the 1970s into the World Wide Web era of the late 1980s and 1990s (Li et al., 2023). Early e-commerce pioneers such as Amazon and eBay transformed retail, while the proliferation of social networks and the smartphone revolution expanded digital touchpoints, introducing both unprecedented convenience and new security risks—ranging from insecure APIs to massive data breaches (Nwankwo et al., 2018; Nwankwo et al., 2022a). Today, the value of global online transactions exceeds five trillion dollars annually and the cost of cybercrime was projected to cost the world about 9.5 trillion US. Dollars in 2024 (Acheme et al,2023b; Morgan,2023). Nigeria boasts of over 60 million internet users, underscoring the nation's rapid digital uptake alongside persistent challenges in managing such scale (NITDA, 2023).

In Nigeria, the Federal Government's National Digital Economy Policy (NDEP) and accelerated investments in broadband infrastructure have catalyzed growth in fintech, e-government, and telehealth services (Victor-Ikoh et al., 2022; Nwankwo, Ukhurebor & Ukaoha, 2020). Yet enduring barriers remain: a stark digital divide between urban centers and rural communities limits equitable access; digital literacy initiatives have not kept pace with technology deployment; and overlapping regulations create uncertainty for innovators and enforcement bodies alike (Adetunji et al., 2022a; Nwankwo et al., 2023a). Meanwhile, Nigeria ranks among the top ten African nations most affected by cybercrime, with ransomware attacks on critical infrastructure and widespread online fraud eroding public trust (Acheme et al,2023b, Irughe et al,2022, Acheme et al,2023a). Through a narrative analysis of Nigeria's digital-economy security landscape, this paper explores how a holistic strategy—blending targeted infrastructure upgrades, cohesive policy reform, robust capacity-building programs, and advanced cybersecurity measures—can unlock inclusive growth, foster resilience, and secure a sustainable digital future for all citizens.

1.1 Secure Digital Economy Components

A secure digital economy rests on the bedrock of resilient digital infrastructure—high-speed broadband networks, scalable data centers, and cloud platforms hardened by multilayered security controls—that enable every subsequent layer of economic activity to function with integrity. Within this fortified environment, e-commerce platforms safeguard buyer and seller interactions through end-to-end encryption and compliance with payment-card industry standards, while digital payment systems—from mobile wallets to tokenized cryptocurrencies—leverage multi-factor authentication and distributed-ledger technology to guarantee transaction authenticity (Nwankwo & Olayinka, 2019). Sophisticated data-analytics pipelines, underpinned by robust data-governance frameworks and privacy-enhancing techniques, extract actionable insights without compromising individual confidentiality, and digital services such as streaming, cloud storage, and SaaS are delivered via secure software-development lifecycles and protected APIs.

The rapid expansion of the Internet of Things—interconnecting devices across homes, industries, and smart cities—brings unprecedented automation and convenience but also heightens the need for zero-trust architectures and continuous firmware patching to thwart device-level exploits (Olayinka et al., 2022;

Nwankwo, Adetunji & Olayinka, 2022). At the same time, artificial intelligence and machine-learning systems drive personalization and operational efficiency while requiring adversarial testing and secure model-training environments to defend against data-poisoning and model-theft attacks (Acheme et al., 2023b; Igulu et al., 2022). Digital marketing relies on encrypted analytics platforms that respect user privacy, and online education portals democratize learning globally with secure identity management and protected content delivery (Nwankwo, 2018). Equally critical are digital government services—ranging from e-taxation to e-licensing—where unified identity frameworks, rigorous access controls, and adherence to international standards such as ISO 27001 ensure that citizen interactions remain both efficient and trustworthy (Nwankwo, Olayinka & Benson,2019). Together, these interwoven components—each reinforced by continuous monitoring, incident-response planning, and privacy-by-design principles—forge a secure digital-economy landscape that fosters innovation, builds public confidence, and underpins sustainable growth.

1.2 Digital Economy in Africa

Africa's digital economy has entered a phase of sustained expansion, driven by surging internet access and smartphone adoption that are unlocking new digital services and e-commerce platforms across the continent. Innovations in mobile money and fintech—underpinned by secure encryption standards and multi-factor authentication—have leapfrogged traditional banking models to deliver financial services to millions of previously underserved users. Innovation hubs and startup ecosystems in cities such as Lagos, Johannesburg, Nairobi, Cairo, and Accra are catalyzing home-grown solutions, while governments are rolling out policies to strengthen broadband networks and incentivize private-sector investment in digital infrastructure.

Yet this rapid growth also brings a complex security landscape that demands proactive measures. To safeguard transactions on Nigeria's bustling e-commerce sites, South Africa's online services, Kenya's pioneering mobile-payment networks, Egypt's digital banking portals, and Ghana's fintech platforms, stakeholders must embed security-by-design principles at every layer—from zero-trust network architectures and end-to-end encryption to rigorous data-protection regulations and real-time threat monitoring. Public-private partnerships for threat-intelligence sharing, comprehensive cybersecurity training programs, and harmonized legal frameworks will be critical to preserve user trust, fortify digital ecosystems against evolving cyber threats, and ensure that Africa's digital transformation proceeds on a foundation of resilience and inclusivity.

1.3 Nigeria's Digital Economy Landscape and Cyber Security

Nigeria's secure digital economy landscape is defined by a convergence of demographic strength, expanding connectivity, and a maturing regulatory environment that emphasizes resilience and trust. With over 60 million internet users as of 2023 (Internet World Stats, 2024) and smartphone penetration accelerating in both urban and rural regions, digital commerce has flourished—from online marketplaces safeguarding transactions with PCI DSS compliant gateways to fintech innovators deploying biometric backed mobile wallets under the oversight of the Central Bank of Nigeria's sandbox framework (Victor Ikoh et al., 2022). This burgeoning ecosystem of tech hubs in Lagos and Abuja has attracted venture capital and fostered home grown solutions in health tech, agri tech, and ed tech, all built atop a foundation of multi layered cybersecurity protocols informed by the Nigeria Data Protection Regulation (2019) and the Cybercrimes Act (2015) (Nwankwo et al., 2020). Yet challenges persist: uneven broadband deployment continues to expose rural communities to service denial attacks, while fragmented digital identity schemes complicate universal access and raise the stakes for fraud and identity theft (Adetunji et al., 2022; Nwankwo et al., 2023).

The agriculture sector—where one in eight Nigerians faced acute hunger in 2023 (Okojie & Odifa, 2023)—illustrates both the promise and the risk of digitization. Precision agriculture pilots using IoT sensors and satellite analytics have demonstrated yield boosts of up to 30 percent by enabling data driven irrigation scheduling and pest surveillance (Olayinka et al., 2022). Secure blockchain enabled traceability platforms have begun to curtail supply chain fraud and post-harvest losses, but their rollout remains uneven outside major commercial farms, leaving smallholders vulnerable to market manipulation exploits. Early warning

systems leveraging cloud-based drought forecasting models can reduce climate driven crop failures, yet their efficacy hinges on robust API security and real time incident response capabilities—areas where underinvestment still leaves gaps (von Grebmer et al., 2021; FAO et al., 2021).

Building a resilient digital economy landscape in Nigeria therefore demands holistic action: accelerating fiber backbone expansion with service level agreements that mandate uptime and encrypted tunnels; harmonizing digital identity frameworks to enable secure single sign on across public and private services; upskilling a broad spectrum of stakeholders through accredited cybersecurity training; and embedding privacy by design and threat modeling into every stage of platform development. Only by weaving security into the very DNA of infrastructure, transactions, and data flows can Nigeria unlock inclusive growth, protect its most vulnerable citizens from hunger and cyber harm, and cement its position as a leading secure digital economy in Africa.

1.4 Digital Economy and Socio-economic Issues

Nigeria has an unemployment rate of 33.3% (See Figure 1-2). The number of poor people in Nigeria is expected to rise from 82.9 million in 2019 to 90 million in 2022 implying that about 45% of the Nigerian population would be living in poverty in 2022(Tade,2021). If USD 3.20 per day is used as a benchmark as proposed, 70% of Nigerians would be considered to be living in poverty (NBS,2020). Isn't that scary? Hunger, poverty, and unemployment are major travails of any economy including most countries in the sub-Saharan Africa, Asia, and Latin America.

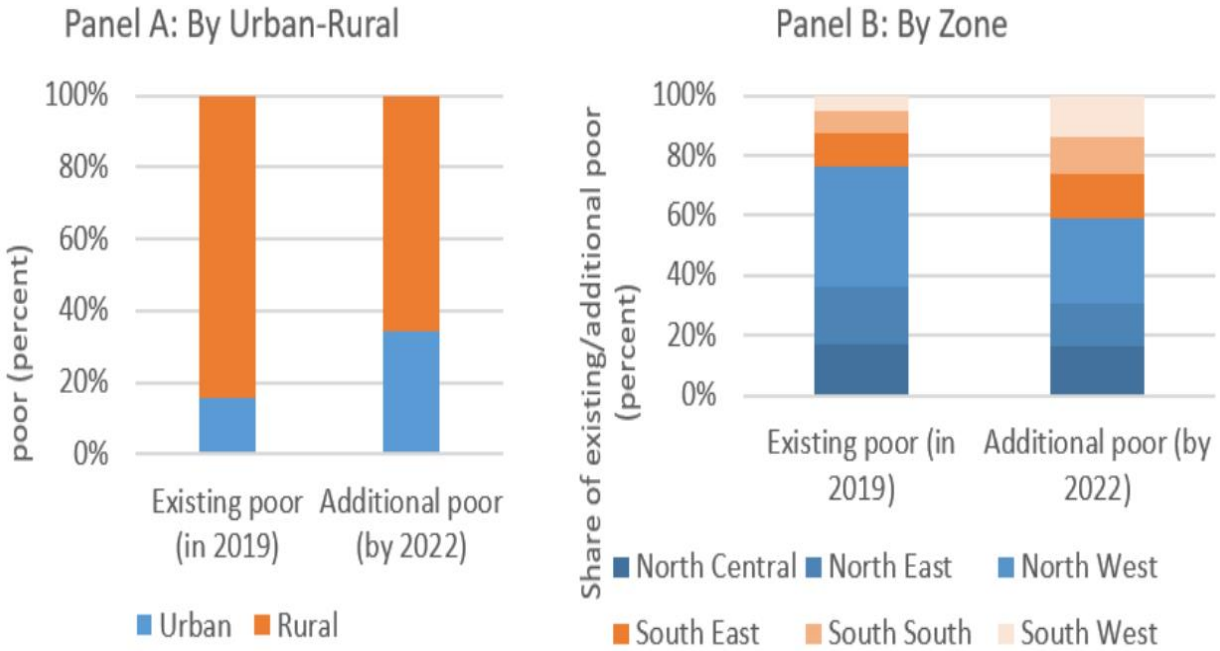

Figure 1: Nigeria's poverty distribution [National Bureau of Statistics, 2020]

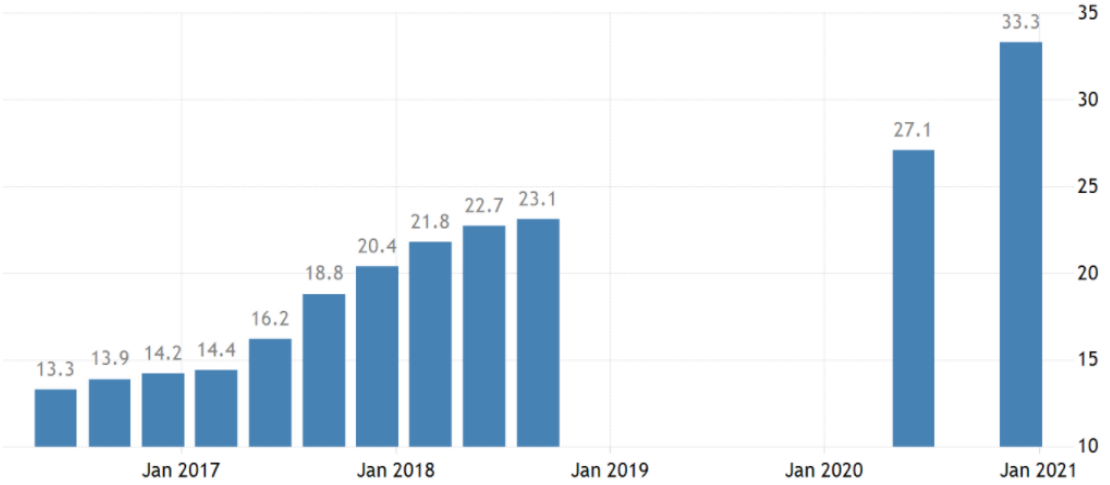

Figure 2: Unemployment in Nigeria [National Bureau of Statistics, 2020]

Job Creation

Digital economy has the capacity to create new types of jobs that revolve around emerging technologies, such as software development, data analysis, digital marketing, e-commerce, and cyber security. As industries adopt digital tools and platforms, they often require skilled professionals to manage and leverage these technologies effectively.

Entrepreneurship and Innovation

The digital economy lowers barriers to entry for entrepreneurs and small businesses. Online platforms and e-commerce allow individuals to start businesses with relatively low upfront costs. This can lead to the creation of new jobs and economic growth.

Remote Work and Flexibility

Digital technologies enable remote work and flexible arrangements, allowing people to work from different locations. This can be especially beneficial for individuals who might have faced barriers to traditional employment due to geographical constraints, disabilities, or caregiving responsibilities.

Gig Economy Opportunities

Digital economy has given rise to the gig economy, where individuals can offer their skills and services on online platforms. While this can sometimes lead to precarious work, it also provides flexible earning opportunities for those who might not be able to participate in traditional full-time employment.

Nigeria's secure digital economy landscape has evolved into an interconnected ecosystem in which advancements in security, environmental stewardship, governance, enterprise growth, resource management, and education are woven together to deliver resilience and inclusion. At the forefront of this transformation are AI driven surveillance networks and IoT sensor arrays that enable real time tracking and behavioral analytics—tools once reserved for high security installations now monitor illicit movements of persons and assets, detect anomaly patterns in transportation corridors, and provide law enforcement agencies with encrypted intelligence feeds to preempt kidnappings or armed robberies (Olayinka et al., 2022). Simultaneously, blockchain anchored payment rails and biometric secured mobile money platforms have neutralized many of the anonymity benefits once enjoyed by ransom seeking criminals, replacing cash based remittances with fully auditable digital trails that law enforcement and financial regulators can trace instantaneously (Nwankwo et al., 2023).

At the same time, the agriculture sector—where one in eight Nigerians faced acute hunger in 2023—has embraced precision farming pilots integrating satellite imagery, edge computing nodes, and AI powered yield prediction models to optimize irrigation schedules and pesticide applications, boosting smallholder productivity by over 25 percent in early trials (Okojie & Odifa, 2023; von Grebmer et al., 2021). These same digital platforms incorporate blockchain based provenance systems, guaranteeing full traceability from farm to fork and curbing post-harvest losses that once exceeded 30 percent in perishable goods. Cloud

hosted drought forecasting applications and mobile warning systems now deliver real time alerts to rural communities, while smart meter networks in urban water utilities apply predictive analytics to detect leaks and unauthorized withdrawals—ion exchange sensors in key pipelines continuously feed data into national water management dashboards, enhancing allocation equity and conservation efforts.

Environmental gains extend beyond agriculture to industrial and civic domains. The embrace of remote work modalities—accelerated by 5G roll outs and secure virtual desktop infrastructures—has slashed daily commuter volumes, reducing carbon emissions by an estimated 12 percent in major metropolitan areas (Adetunji et al., 2022). Government and corporate offices alike have migrated to paper free workflows, cutting document printing costs by millions of naira and preserving forest cover through sustained declines in paper consumption. In manufacturing, IoT enabled energy management platforms optimize equipment runtimes, dynamically adjusting operations to off peak tariffs and renewable energy availability, thereby lowering pollution and operational expenses.

Corruption—which has historically eroded trust in public institutions—is now being countered through e governance initiatives built on transparency by design. Unified digital identity frameworks facilitate secure single sign on for citizens accessing licensing, tax filing, and social welfare services, eliminating hundreds of thousands of face-to-face transactions where graft once thrived. Real time audit trails, mandatory multi-party approval workflows, and publicly accessible dashboards expose each step-in contract awards and fund disbursements, while anonymous whistle blower portals empower civic oversight without fear of reprisal (FAO et al., 2021).

Small and medium sized enterprises (SMEs) have become primary drivers of digital innovation and job creation, leveraging cloud native e marketplaces and AI augmented marketing tools to target customers across Africa and the diaspora. Competitive grants administered via smart contract platforms have funded thousands of start-ups in health tech, fintech, and ed tech, each vetted through algorithmic credit scoring models that broaden access to capital for underbanked entrepreneurs. The agility of these digital SMEs has fostered an ecosystem of collaboration, where industry academic partnerships pilot emerging technologies—such as low cost unmanned aerial vehicles for crop monitoring or open-source health record platforms for rural clinics—under secure development lifecycles and continuous integration pipelines.

Education has likewise been transformed by a surge in immersive and adaptive learning environments. Virtual reality laboratories, secured behind comprehensive identity and access management systems, grant students anywhere the chance to conduct chemistry experiments or network security drills without physical infrastructure. AI driven tutoring bots embedded in national learning management systems provide 24/7 support, identifying at risk learners through predictive analytics and deploying personalized remediation modules in real time. Crucially, these platforms operate under strict data privacy protocols and end to end encryption, ensuring that student records remain confidential and protected against unauthorized access.

Together, these converging trends illustrate how Nigeria's digital economy is no longer a collection of isolated innovations but a cohesive, security centered ecosystem. By embedding security by design at every layer—from secure hardware and zero trust networks to immutable ledgers and privacy preserving analytics—the nation is charting a path toward inclusive growth, hunger reduction, environmental sustainability, and robust governance. As these digital foundations mature, they unlock new avenues for prosperity while safeguarding citizens against both physical and cyber threats, firmly establishing Nigeria as a leader in the secure digital economy landscape of Africa.

2. Literature Review

2.1 Fears Introduced by Digital economy

Nigeria's rapid embrace of digital technologies has undeniably catalyzed new avenues for commerce, communication, and innovation, but it has also surfaced a host of interrelated anxieties that must be addressed to ensure a truly inclusive and resilient digital economy. The enduring digital divide in Nigeria—where reliable broadband remains unaffordable or unavailable for many rural and peri-urban communities—risks entrenching existing socioeconomic disparities, as those without access are shut out from e-learning, telemedicine, and digital marketplaces. Simultaneously, the relentless march of

automation and AI-powered platforms threatens to displace workers across agriculture, manufacturing, and administrative sectors; the rise of algorithmic job-matching in the gig economy offers flexibility, yet those roles often lack the social protections and stable incomes that traditional employment once provided, deepening inequality for those without advanced digital skills (ILO, 2023).

At the same time, cybersecurity threats have grown in both sophistication and volume, from ransomware attacks that can paralyze hospital networks and municipal services to supply-chain exploits targeting critical infrastructure—incidents that erode public confidence in online financial systems and digital government portals under the Nigeria Data Protection Regulation (2019) and Cybercrimes Act (2015). The proliferation of generative-AI tools has accelerated the spread of deepfakes and targeted disinformation campaigns via social media channels, stoking social unrest and complicating election integrity efforts (UNESCO, 2022). Unregulated online platforms can serve as conduits for illicit activities—ranging from human trafficking to cyber-fraud—exacerbating national security concerns and imposing new burdens on law enforcement to monitor encrypted communication networks.

Environmental and systemic risks compound these socioeconomic and security fears. Nigeria now generates hundreds of thousands of tons of e-waste annually, much of it informally recycled or dumped, releasing toxic heavy metals into soil and waterways (UN E-waste Monitor, 2023). Meanwhile, the data centers powering cloud services, AI workloads, and 5G trials are voracious energy consumers; in regions still dependent on gas and diesel generators, their carbon footprint is climbing even as global power grids decarbonize (IEA, 2024). The extraction of rare minerals for smartphones and servers contributes to deforestation and water pollution, underscoring the need for sustainable supply-chain standards. Furthermore, systemic reliance on digital infrastructure exposes entire sectors to service outages—whether due to cyberattacks, equipment failures, or natural disasters—highlighting the critical importance of resilient network architectures and robust disaster-recovery planning.

Confronting these multifaceted fears demands a holistic strategy: investing in universal broadband access and digital-literacy programs to narrow the divide; enacting labour policies that guarantee social protections for automated and gig-economy workers; mandating cybersecurity frameworks with continuous-monitoring requirements; expanding e-waste recycling and green-energy incentives for data centres; and strengthening regulatory oversight to deter disinformation and illicit online activity. Only by weaving together economic, social, environmental, and governance measures can Nigeria transform these digital-economy fears into opportunities for sustainable, secure, and equitable growth.

Nigeria’s rapid embrace of digital technologies has undeniably catalyzed new avenues for commerce, communication, and innovation, but it has also surfaced a host of interrelated anxieties that must be addressed to ensure a truly inclusive and resilient digital economy. The enduring digital divide in Nigeria—where reliable broadband remains unaffordable or unavailable for many rural and peri-urban communities—risks entrenching existing socioeconomic disparities, as those without access are shut out from e-learning, telemedicine, and digital marketplaces. Simultaneously, the relentless march of automation and AI-powered platforms threatens to displace workers across agriculture, manufacturing, and administrative sectors; the rise of algorithmic job-matching in the gig economy offers flexibility, yet those roles often lack the social protections and stable incomes that traditional employment once provided, deepening inequality for those without advanced digital skills (ILO, 2023).

At the same time, cybersecurity threats have grown in both sophistication and volume, from ransomware attacks that can paralyze hospital networks and municipal services to supply-chain exploits targeting critical infrastructure—incidents that erode public confidence in online financial systems and digital government portals under the Nigeria Data Protection Regulation (2019) and Cybercrimes Act (2015). The proliferation of generative-AI tools has accelerated the spread of deepfakes and targeted disinformation

campaigns via social media channels, stoking social unrest and complicating election integrity efforts (UNESCO, 2022). Unregulated online platforms can serve as conduits for illicit activities—ranging from human trafficking to cyber-fraud—exacerbating national security concerns and imposing new burdens on law enforcement to monitor encrypted communication networks.

Environmental and systemic risks compound these socioeconomic and security fears. Nigeria now generates hundreds of thousands of tons of e-waste annually, much of it informally recycled or dumped, releasing toxic heavy metals into soil and waterways (UN E-waste Monitor, 2023). Meanwhile, the data centers powering cloud services, AI workloads, and 5G trials are voracious energy consumers; in regions still dependent on gas and diesel generators, their carbon footprint is climbing even as global power grids decarbonize (IEA, 2024). The extraction of rare minerals for smartphones and servers contributes to deforestation and water pollution, underscoring the need for sustainable supply-chain standards. Furthermore, systemic reliance on digital infrastructure exposes entire sectors to service outages—whether due to cyberattacks, equipment failures, or natural disasters—highlighting the critical importance of resilient network architectures and robust disaster-recovery planning.

Confronting these multifaceted fears demands a holistic strategy: investing in universal broadband access and digital-literacy programs to narrow the divide; enacting labour policies that guarantee social protections for automated and gig-economy workers; mandating cybersecurity frameworks with continuous-monitoring requirements; expanding e-waste recycling and green-energy incentives for data centres; and strengthening regulatory oversight to deter disinformation and illicit online activity. Only by weaving together economic, social, environmental, and governance measures can Nigeria transform these digital-economy fears into opportunities for sustainable, secure, and equitable growth.

2.2 Grassroots Secure Digital Economy Implementation in Nigeria

In Nigeria's quest for a secure digital economy, the most profound impediment remains the uneven quality and reach of foundational infrastructure—a gap that particularly hobbles grassroots communities. Major cities have seen fibre-optic rollouts, 4G expansions and even early 5G trials, yet in countless rural areas connectivity still depends on weak 3G signals and sporadic satellite links, compounded by data prices that many low-income households cannot afford. Even where the internet is available, chronic power instability forces small businesses and community telecentres to rely on noisy diesel generators or costly solar-battery systems, driving up the true cost of "going digital." Meanwhile, Nigeria's burgeoning data-center scene—anchored by large Lagos and Abuja facilities—is largely absent from the country's northern and coastal regions, depriving local entrepreneurs of low-latency edge computing and forcing them to host sensitive information offshore under less restrictive security regimes.

This patchy infrastructure also amplifies cybersecurity risks: without resilient, encrypted backbones and local hosting, grassroots users are exposed to man-in-the-middle attacks on public Wi-Fi, phishing campaigns via unstable mobile networks, and data-soaking malware in unpatched systems. Compounding these technical challenges is a yawning skills gap—despite a surge in coding bootcamps, university hackathons, and government-sponsored digital literacy programs, many Nigerians lack the training needed to configure secure endpoints, deploy basic firewalls, or recognize social-engineering ploys.

Logistics networks for e-commerce remain similarly uneven. While drone delivery pilots for medical supplies in remote regions have garnered headlines, most small vendors still contend with inflated last-mile shipping fees, poor road conditions, and insecure drop-off points that undermine customer trust. Payment rails have improved—CBN's instant-payment gateway (NIP), USSD wallets, and biometric-anchored mobile-money services have driven financial inclusion to new heights—but unreliable network links and fragmented KYC processes hinder real-time fraud detection and end-to-end encryption compliance at the grassroots.

Regulatory frameworks—like the Nigeria Data Protection Regulation, the Cybercrimes Act, and the CBN's sandbox initiative—offer blueprints for a secure ecosystem, yet their implementation remains concentrated in formal sectors. Without interoperable API standards and a unified digital-identity framework extending from NIMC's national ID to local SIM registration, small-scale farmers, artisans, and micro-enterprises cannot seamlessly tap into e-government services or participate in secure value chains.

Closing these gaps will require a coordinated push: subsidized community broadband and solar-microgrid projects to stabilize power and connectivity; proliferation of micro data centers and edge nodes under green-energy mandates; scaled cybersecurity training tied to local language outreach; last-mile logistics hubs powered by electric vehicles; and an agile regulatory sandbox that brings digital-ID, KYC, and data-protection standards down to the grassroots. Only by embedding security-by-design into every layer of infrastructure and skills development can Nigeria transform its vast potential into an inclusive, resilient, and truly secure digital economy.

2.3 Cybersecurity Concerns

Cybersecurity plays a crucial role in shaping the digital economy. By safeguarding digital assets, sensitive data, and online transactions, it instills trust and confidence in consumers and businesses, encouraging their active participation in the digital ecosystem (Daniel et al,2021, Acheme et al,2023b; Nwankwo et al,2022a; Irughe et al,2022). A robust cybersecurity framework protects against cyber threats like data breaches, ransomware attacks, and identity theft, preventing potential economic losses and disruptions to businesses.

Furthermore, cyber threats can deter investors and hinder the growth of digital businesses, making a strong cybersecurity posture essential for fostering innovation and attracting investments in the digital economy. As more industries embrace digital transformation, the need for cybersecurity becomes even more significant to protect critical infrastructure and ensure the uninterrupted functioning of essential services.

Ultimately, a secure digital environment fosters economic growth, as consumers and businesses are more likely to engage in e-commerce, online transactions, and digital services when they have confidence that their data and assets are well-protected. As such, investing in cybersecurity measures becomes a strategic imperative to ensure the sustainability and prosperity of the digital economy. The rising number of cyber threats and the lack of robust cybersecurity measures pose significant risks to digital transactions and data privacy.

2.4 Digital Literacy Gap

The lack of digital literacy among a significant portion of the population hinders effective digital engagement and adoption of digital services. Nigeria faces a digital literacy gap, as there is a disparity in digital skills and access to technology between different segments of the population. This gap was influenced by factors such as socioeconomic status, education levels, and geographical location. It's essential to address this issue to ensure equitable access to digital opportunities and to promote inclusive development.

2.5 Regulatory Frameworks

Ambiguities and complexities in any regulatory environment will create uncertainty for businesses and investors in the digital space (Onatuyeh et al,2025). Nigeria's digital economy is confronted with various regulatory challenges. Some of the key issues include:

a. Lack of comprehensive legislation: Nigeria's digital economy lacked specific regulations tailored to address the unique challenges of the digital space, leading to uncertainty and ambiguities in certain areas.

b. Data privacy and protection: Data privacy laws were not well-defined, leaving personal data vulnerable to misuse and unauthorized access. This raised concerns about consumer trust and cybersecurity.
c. E-commerce regulations: The absence of comprehensive e-commerce regulations sometimes resulted in disputes between online businesses and consumers, impacting the growth of the digital marketplace.
d. Payment systems and digital financial services: The regulatory framework for digital payment systems and FinTech services was still evolving, affecting the adoption and growth of digital financial services.
e. Taxation and revenue collection: The taxation of digital services and cross-border transactions posed challenges, as it was difficult to monitor and collect taxes from digital businesses effectively.

3. Proposed Solutions

To transform Nigeria's digital-economy ambitions into secure, inclusive reality, policymakers and stakeholders must orchestrate a coordinated push across infrastructure, regulation, skills, and sustainability. First, accelerating the National Broadband Plan—bolstered by recent expansions of submarine cables (e.g., WACS) and 5G trials by major operators—will bring affordable, low-latency connectivity to rural and peri-urban communities, while off-grid solar-hybrid microgrids can stabilize power for telecentres, clinics, and SMEs. At the same time, local edge-data centers, built under Nigeria's new Cloud Computing Policy, should be incentivized with green-energy credits to host sensitive data onshore, reducing reliance on distant servers and cutting backhaul vulnerabilities.

Regulatory reform must follow in lockstep. The pending Digital Identity Bill—by unifying NIN, SIM-registration, and eKYC processes—will enable secure single sign-on for citizens across e-government portals, fintech apps, and health platforms. Expanding the Central Bank's sandbox framework to include agritech and e-logistics innovations will fast-track home-grown solutions in precision-farming and last-mile delivery, while mandating baseline cybersecurity standards (aligned to ISO 27001 and the Nigeria Data Protection Regulation) will enforce continuous monitoring, incident-response drills, and regular third-party audits. Cross-border cooperation through ECOWAS and INTERPOL channels will strengthen threat-intelligence sharing against transnational cybercrime and network-based attacks.

On the human front, embedding digital-literacy curricula from primary schools through community-based "Tech Hubs" will ensure Nigerians can configure secure endpoints, spot phishing attempts, and manage privacy settings. Accredited bootcamps—partnering with global cloud providers and cybersecurity firms—can certify thousands of new DevSecOps engineers, while mobile-first "learning-on-the-go" apps will reach remote farmers and artisans. For agricultural communities, government-NGO–NGO alliances can deploy IoT-enabled soil-moisture sensors and blockchain traceability pilots, coupled with fintech microcredit tied to digital wallets, to boost yields, curb post-harvest losses, and guarantee transparent payment flows.

Environmental stewardship must also be baked in. Manufacturers take-back schemes and formal e-waste recycling parks—supported by Extended Producer Responsibility mandates—will prevent hazardous dumps. Data centres and telecom towers should qualify for renewable-energy subsidies, and a circular-economy roadmap for electronics (emphasizing repair, refurbishment, and material recovery) will conserve scarce resources. Finally, embedding "privacy-by-design" and "security-by-design" into every new platform—from e-commerce marketplaces to digital-health systems—will ensure that as Nigeria's digital economy scales, it remains resilient against both cyber-threats and the very real social, environmental, and governance challenges at its grassroots.

4. Conclusion

The journey towards a secure digital economy in Nigeria is both a monumental challenge and an unparalleled opportunity. Our analysis has shown that without resilient broadband networks and reliable power, even the most innovative fintech or agritech solutions will falter; without a workforce equipped with cybersecurity awareness and advanced digital skills, every portal—be it for e-government or e-commerce—remains vulnerable to compromise; and without coherent, forward-looking regulations that embed privacy-by-design and security-by-design at their core, trust in digital platforms will never fully materialize. Yet, as this paper has demonstrated, these obstacles are surmountable through a concerted, multi-stakeholder commitment: accelerating edge-data center deployment under green-energy mandates; unifying digital-identity schemes to underpin secure single-sign-on; scaling accredited DevSecOps training to fortify human capital; and enriching the policy landscape with agile sandboxes and international threat-intelligence partnerships.

By embracing these integrated strategies—rooted in global best practices yet tailored to Nigeria's unique socioeconomic tapestry—the nation can not only bridge its digital divide and inoculate its digital assets against evolving threats but also unleash the latent potential of its entrepreneurs, farmers, educators, and public servants. In doing so, Nigeria will position itself as a beacon of innovation and resilience in Africa's digital economy, charting a course toward sustainable prosperity that leaves no citizen behind and solidifies the country's role as a regional leader in secure, inclusive digital transformation.

Acknowledgements

Conflict of Interest

The authors declared no conflict of interest.

References

Acheme, I. D., Nwankwo, W., Olayinka, A. S., Makinde, A. S., & Nwankwo, C. P. (2023a). Petroleum drilling monitoring and optimization: Ranking the rate of penetration using machine learning algorithms. In Z. Hu, Q. Zhang, & M. He (Eds.), *Advances in artificial systems for logistics engineering III* (Lecture Notes on Data Engineering and Communications Technologies, Vol. 180). Springer. https://doi.org/10.1007/978-3-031-36115-9_15

Acheme, S.O., Nwankwo, W., Acheme, D., Nwankwo, C.P. (2023b). A Crypto-Stego Distributed Data Hiding Model for Data Protection in a Single Cloud Environment. In: Hu, Z., Wang, Y., He, M. (eds) Advances in Intelligent Systems, Computer Science and Digital Economics IV. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 158. Springer, Cham. https://doi.org/10.1007/978-3-031-24475-9_38

Adetunji, C. O., Nwankwo, W., Olayinka, A. S., Olaniyan, O. T., Akram, M., Laila, U., Olugbenga, M. S., Oshinjo, A. M., Adetunji, J. B., Okotie, G. E., & Esiobu, N. (2022a). Machine learning and behaviour modification for COVID-19. In H. M. Inuwa, I. M. Ezeonu, C. O. Adetunji, E. O. Ekundayo, A. Gidado, A. B. Ibrahim, & B. E. Ubi (Eds.), *Medical biotechnology, biopharmaceutics, forensic science and bioinformatics* (pp. 271–287). Taylor & Francis.

Adetunji, C. O., Olaniyan, T. O., Osikemekha, A. A., Daniel, I. H., Nwankwo, W., Olayinka, A. S., & Ukhurebor, K. E. (2022b). Cyberespionage: Socioeconomic implications on sustainable food security. In A. Abraham, S. Dash, J. J. P. C. Rodrigues, B. Acharya, & S. K. Pani (Eds.), *Intelligent data-centric systems: AI, edge and IoT-based smart agriculture* (pp. 477–486). Academic Press. https://doi.org/10.1016/B978-0-12-823694-9.00011-6

Alola, A. A., Muoneke, O. B., Okere, K. I., & Obekpa, H. O. (2023). Analysing the co-benefit of environmental tax amidst clean energy development in Europe's largest agrarian economies. *Journal of Environmental Management, 326*, 116748.

Amanullah, A., Lakhan, G. R., Channa, S. A., Magsi, M., Koondher, M. A., Wang, J., & Channa, N. A. (2020). Credit constraints and rural farmers' welfare in an agrarian economy. *Heliyon*, *6*(10), e05252.

Bueno, D. (2019). Genetics and learning: How the genes influence educational attainment. *Frontiers in Psychology*, *10*, 1622. https://doi.org/10.3389/fpsyg.2019.01622

Daniel, A., Shaba, S. M., Momoh, M. O., Chinedu, P. U., & Nwankwo, W. (2021). A computer security system for cloud computing based on encryption technique. *Computer Engineering and Applications*, *10*(1), 41–53.
Food and Agriculture Organization of the United Nations. (2021). *The state of food security and nutrition in the world 2021*. FAO.

Igulu, K. T., Nwankwo, W., Palimote, J., & Onuodu, F. (2022). Algorithms for robotics position and navigation. In T. Singh, N. Singh, & B. Azzoparti (Eds.), *Advances in autonomous navigation through intelligent technologies*. CRC Press.

Irughe, D. U., Nwankwo, W., Nwankwo, C. P., & Uwadia, F. (2022). Resilience and security on enterprise networks: A multi-sector study. 2022 5th Information Technology for Education and Development (ITED), 1–7. https://doi.org/10.1109/ITED56637.2022.10051458.

Li, T., Zhang, Y., Bi, X., Wu, J., Chen, M., Luo, B., & Feng, Y. (2023). Comprehensive performance evaluation of coordinated development of industrial economy and its air pollution control. *Heliyon*, *9*(7), e17442.

Momoh, M. O., Chinedu, P. U., Nwankwo, W., Aliu, D., & Shaba, M. (2021). Blockchain adoption: Applications and challenges. *International Journal of Software Engineering and Computer Systems, 7*(2), 19–25. https://doi.org/10.15282/ijsecs.7.2.2021.3.0086

Morgan,S.(2023). Cybercrime To Cost The World $9.5 trillion USD annually in 2024. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

National Bureau of Statistics. (2020). *Poverty and inequality in Nigeria*. National Bureau of Statistics.

Nwankwo, C., Adigwe, W., Nwankwo, W., Kizito, A. E., Konyeha, S., & Uwadia, F. (2022b). An improved password-authentication model for access control in connected systems. In 5th Information Technology for Education and Development (ITED) (pp. 1–8). IEEE. https://doi.org/10.1109/ITED56637.2022.10051179

Nwankwo, C., Uwadia, F., Nwankwo, W., Adigwe, W., Chinedu, P., & Ojei, E. (2022a). Privacy and security of content: A study of user-resilience and pre-checks on social media. In 5th Information Technology for Education and Development (ITED) (pp. 1–8). IEEE. https://doi.org/10.1109/ITED56637.2022.10051589

Nwankwo, W. (2018). Promoting equitable access to university education through online learning systems. *World Journal of Engineering Research and Technology*, *4*(2), 517–543.

Nwankwo, W., Olanrewaju, B., Chinedu, P. U., & Olayinka, C. (2018). National social information technology infrastructure: A potent mechanism for waging anti-corruption war. *American Journal of Embedded Systems and Applications, 6*(1), 56–68.

Nwankwo, W. & Olayinka, A.S.(2019). Implementing a risk management and X-Ray cargo scanning document management prototype, *International Journal of Scientific and Technology Research*, 8(9),93-105.

Nwankwo, W., & Njoku, C. C. (2019). Adoption of internet voting platform: Containing data injection threats with structured LINQ. *Nigerian Research Journal of Engineering and Environmental Sciences*, *4*(2), 724–739.

Nwankwo, W., Olayinka, A. S., & Benson, B. U. (2019). X-ray cargo scanning and risk management in trade facilitation: Analysis and model of an online imaging and documentation management system. *International Journal of Modern Education and Computer Science, 11*(5), 10–23. https://doi.org/10.5815/ijmecs.2019.05.02

Nwankwo, W., Ukhurebor, K. E., & Ukaoha, K. C. (2020). Knowledge discovery and analytics in process re-engineering: A study of port clearance processes. In 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS) (pp. 1–7). IEEE. https://doi.org/10.1109/ICMCECS47690.2020.246989

Nwankwo, W., Umezuruike, C., & Njoku, C. C. (2020). Enhancing learning systems using interactive intelligent components. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(3), 3390–3397.

Nwankwo, W., Adetunji, C. O., Olayinka, A. S., Ukhurebor, K. E., Ukaoha, K. C., Umezuruike, C., Chinedu, P. U., & Benson, B. U. (2021). The adoption of AI and IoT technologies: Socio-psychological implications in the production environment. *IUP Journal of Knowledge Management, 19*(1), 50–75.
Nwankwo, W., Chinedu, P. U., Aliu, D., Saliu, M. S., Momoh, M. O., Nwankwo, C. P., & Adigwe, W. (2022). Integrated fintech solutions in learning environments in the post-COVID-19 era. *IUP Journal of Knowledge Management, 20*(3), 1–22.

Nwankwo, W., Nwankwo, C. P., & Adigwe, W. (2022). Leveraging on artificial intelligence to accelerate sustainable bioeconomy. *IUP Journal of Knowledge Management, 20*(2), 38–59.

Nwankwo, W., Chinedu, P. U., Masajuwa, F. U., Njoku, C. C., & Imoisi, S. E. (2023). Adoption of i-voting infrastructure: Addressing network-level cybersecurity breaches. *E-Government: An International Journal, 19*(3), 273–303. https://doi.org/10.1504/EG.2023.130582

Nwankwo, W., Chinedu, P. U., Aliu, D., Saliu, M. B., Momoh, M. O., Nwankwo, C. P., Adigwe, W., Oghorodi, D., & Uwadia, F. (2023). Educational fintech: Promoting stakeholder confidence through automatic incidence resolution. In Z. Hu, Y. Wang, & M. He (Eds.), *Advances in intelligent systems, computer science and digital economics IV* (Lecture Notes on Data Engineering and Communications Technologies, Vol. 158). Springer. https://doi.org/10.1007/978-3-031-24475-9_78

Olayinka, A. S., Adetunji, C. O., Nwankwo, W., Olugbemi, O. T., & Olayinka, T. C. (2022). A study on the application of Bayesian learning and decision trees IoT-enabled system in postharvest storage. In S. Pal, D. De, & R. Buyya (Eds.), *Artificial intelligence-based internet of things systems* (Internet of Things: Technology, Communications and Computing). Springer. https://doi.org/10.1007/978-3-030-87059-1_18

Okojie, J., & Odifa, D. (2023). Nigeria's hunger levels rising despite agric production push. *Business Day*. Retrieved from https://businessday.ng/agriculture/article/nigerias-hunger-levels-rising-despite-agric-production-push/#:~:text=In%20April%202023%2C%20the%20United,people%20%E2%80%94%20were%20facing%20acute%20hunger

Onatuyeh, E. A., Oghorodi, D., Okpako, E. A., Ojei, E., Osakwe, G., Chinedu, N. B., Okoh, S. K., Odu, V. C., Chinedu, P. U. and Nwankwo, W.(2025). Cybersecurity and Business Survival in Nigeria: Building Customer's Trust. *African Journal of Applied Research*, 11(1),786-813.

Tade, O. (2021). Poverty and widening inequality in Nigeria. *Vanguard*. Retrieved from https://www.vanguardngr.com/2021/07/poverty-and-widening-inequality-in-nigeria/

Victor-Ikoh, M. I., Moko, A., & Nwankwo, W. (2022). Towards the implementation of a versatile mobile health solution for the management of immunization against infectious diseases in Nigeria. In G. Salvendy & J. Wei (Eds.), *Design, operation and evaluation of mobile communications* (Lecture Notes in Computer Science, Vol. 13337). Springer. https://doi.org/10.1007/978-3-031-05014-5_7

von Grebmer, K., Bernstein, J., Wiemers, M., Schiffer, T., Hanano, A., & Towey, O. (2021). *Global hunger index*. Retrieved from https://www.globalhungerindex.org/pdf/en/2021.pdf