FIGHTING CORRUPTION IN NIGERIA: A TECHNOLOGY-DRIVEN APPROACH

SULE SEIDU
Federal University of Technology Babura, Jigawa State, Nigeria
Talk2seidu@gmail.com, 08059288903

ABSTRACT

This paper argues that corruption in Nigeria is a major barrier to development and proposes a technology-driven solution, but one that goes beyond simply buying computers. The core framework combines three theories to explain why anti-corruption technology succeeds or fails. First, the Technology Acceptance Model (TAM) suggests people will only use these tools if they find them genuinely useful (Perceived Usefulness) and easy to use (Perceived Ease of Use). Second, a socio-technical perspective stresses that human and organizational factors are as critical as the technology itself. Third, Institutional Theory explains how outside pressures can either sabotage or support these systems. The study examines tools like e-governance platforms, data management, and secure whistleblower systems to boost transparency and citizen oversight.The key finding is that investing in ICT infrastructure alone is not enough. Success depends entirely on user acceptance and long-term sustainability. Major obstacles include poor infrastructure, a vast digital divide caused by low digital literacy, and the grim paradox of corrupt insiders using the technology itself to commit fraud. The paper concludes that sustainable e-governance requires a security-first culture that focuses on human factors. Its strategic recommendations are to automate processes to remove human discretion, enforce strict information security policies, and design user-friendly interfaces to overcome literacy barriers. The ultimate goal is to transform ICT from a simple tool into a comprehensive ecosystem for integrity and accountability.

Key Words: Corruption, ICT Initiative and ICT Sustainability.

Introduction

Corruption is a global phenomenon, yet its pervasive nature in Nigeria presents a critical developmental challenge. The Transparency International (TI) Corruption Perceptions Index for 2019 ranked Nigeria 146th globally, scoring a mere 26 out of 100, thereby positioning it as the second most corrupt country within the Economic Community of West African States (ECOWAS) (Transparency International, 2020). While globally, Information and Communication Technology (ICT) has been lauded as a potent instrument for curbing corruption by enabling the collection of digital evidence, simplifying processes, and enhancing surveillance (Wickberg, 2013; Krishnan, Teo, & Lim, 2013), its application in Nigeria presents a significant paradox. Rather than solely mediating corrupt practices, ICT systems are often themselves enmeshed in and subverted by the very corruption they are meant to combat (Ogutu, Okello, & Otieno, 2014).

This contradiction stems not from the inherent failure of technology, but from the socio-technical context of its deployment. The value of any technological innovation is a function of its adoption, acceptance, and long-term sustainability (Sahi& Gupta, 2013). In Nigeria, the potential of ICT is undermined by a fundamental lack of valuing these systems as performance-enhancing assets. Instead, ICT is often perceived as a threata corruption-exposing technologyleading to systemic resistance, poor implementation, and the perpetuation of a corrupt value system within the technological sphere. Consequently, increased ICT investment, in the absence of robust adoption and governance frameworks, paradoxically creates new avenues for corruption.

Beyond the challenges of adoption, the efficacy of ICT as an anti-corruption tool is contingent upon a secure and reliable information system architecture. A secure ICT system requires a well-engineered structure encompassing hardware, software, data protocols, and rigorous data governance to ensure the confidentiality, integrity, and availability (CIA triad) of information (Stallings & Brown, 2012). However, the most sophisticated technical safeguards are often compromised by the human element. Users constitute the most significant vulnerability, frequently becoming the weakest link through practices such as weak password management or leaving unencrypted files on unprotected systems (Fenz*et al.,*2014). Therefore, a technology-driven approach to fighting corruption must concurrently address both the macro-level issues of adoption and governance, and the micro-level factors of user behavior and information security.

This study aims to delineate a comprehensive framework of strategies to combat corruption in Nigeria through the effective adoption, acceptance, and secure sustainability of ICT. The primary objective is to synthesize existing knowledge to identify the critical socio-technical barriers that subvert technology's anti-corruption potential and to propose actionable, context-sensitive strategies. This paper seeks to move beyond the technological determinism that often characterizes this discourse, providing a nuanced analysis of how e-governance, data governance, and a secure ICT culture can collectively foster transparency and accountability.

Problem Statement

Despite significant advancements in global information technology, security breaches within ICT innovations in Nigeria continue to proliferate, a trend mirrored by the nation's persistently high corruption levels. The nation's Corruption Perceptions Index has shown a general, albeit fluctuating, increase in corruption, averaging 20.98 points from 1996 to a high of 26 in 2019 (Transparency International, 2020). This correlation is not coincidental; ICT systems intended to be instrumental for transparency are frequently compromised by corrupt policies, unethical practices, and a lack of institutional integrity. The core problem is that the implementation of comprehensive proceduresincluding data governance, e-governance policies, and operational activities designed to mediate corruption and mitigate security threatsis critically deficient. Specifically, many information technology managers and policymakers lack the strategic insight to develop and deploy ICT innovation systems that are resilient to both external threats and

internal subversion. This study addresses the gap between the theoretical potential of ICT for combating corruption and its failed implementation in the Nigerian context.

Literature Review and Synthesis

Corruption and the Technological Imperative

Corruption, as defined by Transparency International, is the abuse of entrusted power for private gain, manifesting in various forms including bribery, embezzlement, and money laundering (Transparency International, 2020). The global consensus, supported by a substantial body of literature, is that transparency and openness are essential for deterring such behaviors. ICT offers unprecedented mechanisms to achieve this through the systematic capture, analysis, and dissemination of information (Wickberg, 2013). A critical mechanism through which ICT can impact corruption is e-governance, defined as the application of ICT and the Internet to facilitate government services and operations, thereby enhancing transparency, accountability, and citizen engagement (Krishnan *et al*., 2013; Ionescu, 2013). Research has demonstrated a significant negative relationship between sustainable e-government and corruption, positioning ICT as a crucial enabler for systemic reform (Güney, 2017). The dynamic and interdependent relationship among ICT, e-governance, and corruption can be conceptualized as a continuous sequence: ICT enables e-governance, e-governance mediates corruption, but corruption can also subvert and plague the very ICT systems meant to counter it, creating a vicious cycle.

Barriers to Implementing Sustainable Anti-Corruption Technology in Nigeria

Despite the theoretical promise, the implementation of effective ICT in Nigeria is stymied by several interconnected barriers, which this study categorizes into three thematic areas.

Systemic Infrastructural and Data Governance Deficits

A primary barrier is the non-existent or poorly implemented ICT infrastructure, characterized by incomplete digital systems and a fundamental misunderstanding of data governance. Data governance refers to the framework of rules, policies, roles, and responsibilities that ensures data is accurate, consistent, complete, available, and secure, treating information as a strategic national asset (Koltay, 2016; Data Governance Institute, 2015). The absence of such a framework in Nigeria means ICT innovations are often reduced to their hardware components, lacking the integrated "information and communication" architecture required for functionality. A salient example is the country’s traffic light systems, which are often deployed with embedded monitoring cameras but remain non-functional, necessitating the manual and corruption-prone intervention of law enforcement officers. This failure is emblematic of a broader issue: the inability to automate processes due to a lack of integrated databases. Without a unified vehicle and driver's license registry, agencies like the Nigeria Road Safety Commission cannot perform real-time verification, creating loopholes for fraud and bribery. This operational environment, where ICT is present but non-functional, breeds cynicism and actively undermines technology adoption and sustainability (Ogutu et al., 2014).

The Digital Divide: Literacy, Trust, and Usability

The high rate of digital illiteracy and a profound lack of trust in technology constitute the second major barrier. With a national literacy rate of only 59.67% for adults (UNESCO, 2015), a significant portion of the Nigerian populace is excluded from e-governance initiatives that are not designed with their needs in mind. This digital divide is compounded by a widespread lack of trust in digital systems. Evidence of this mistrust is stark: a survey by Enhancing Financial Innovation and Access (EFInA) revealed that only 7.9% of Nigerians use ATMs, and an estimated 65% of the country's currency in circulation remains outside the formal banking system (Emengini&Alio, 2014; Itah&Ene, 2014). This behavior is not solely a function of illiteracy but also reflects a deep-seated fear of technology-mediated fraud, a lack of confidence in system reliability, and a preference for cash-based transactions that can facilitate corruption. The failure of existing technological platforms to provide easy-to-use interfaces for the semi-literate and to build trust through consistent, error-free performance is a critical design flaw that perpetuates exclusion and undermines the potential for citizen-led accountability.

Policy Corruption and Institutional Subversion of Technology

The third and most insidious barrier is the deliberate subversion of ICT systems by corrupt policies and practices. ICT innovations, which should operate on objective, rule-based algorithms, are instead corrupted by human emotions and social status, rendering them "useless and with nonsensical outputs." This is evident in the systemic flouting of traffic laws by politically exposed persons who face no technological consequence, and the common use of official government license plates on private vehicles. Such practices represent a direct assault on the integrity of the technological system, demonstrating that enforcement and accountability are selective. When technology is programmed with, or forced to accommodate, "attitude," it loses its objectivity and becomes another instrument of power rather than a tool of transparency. This institutional subversion signals to the public that the rule of law does not apply uniformly, thereby destroying trust in both the state and the technological systems it deploys.

Theoretical Framework

This study is grounded in an integrated theoretical framework, uniting the Technology Acceptance Model (TAM), Institutional Theory, and the socio-technical systems (STS) perspective to provide a multi-level analysis of the ICT-corruption nexus.

At the micro or individual level, the Technology Acceptance Model (TAM), developed by Fred Davis in 1989, posits that two primary variables determine a user's acceptance and use of a technology: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) (Davis, 1989). TAM is predicated on the psychological theories of Reasoned Action and Planned Behavior, providing a robust framework for understanding the complex relationship between system characteristics (external variables) and actual system usage. PU and PEOU are, in turn, shaped by a multitude of factors including cognitive ability (Chen *et al*., 2013), social and cultural influences (Kaushik &

Rahman, 2015), self-efficacy (Teoh*et al.,* 2013), and facilitating conditions (Tsai, 2015). For an anti-corruption technology framework to be successful in Nigeria, it must be perceived as both useful for its intended purpose—enhancing transparency—and easy to use by a citizenry characterized by vast disparities in literacy, income, and technological exposure.

However, TAM alone is insufficient to explain the organizational resistance and systemic subversion observed. To address this, the study integrates Institutional Theory, which examines how institutional environments shape organizational structures and actions through regulative (laws, rules), normative (values, norms), and cultural-cognitive (shared beliefs, symbols) pillars (Scott, 2014). In the Nigerian context, this theory illuminates how corrupt practices become "institutionalized"accepted as the normal, albeit illicit, way of conducting government business. The subversion of ICT systems, such as the non-enforcement of traffic laws for elites, is not merely an individual act of circumvention but a manifestation of a deep-seated institutional logic where power and status override formal rules. This creates mimetic and normative pressures on other actors to also disregard the technology, thereby explaining the "paradox" of ICT being used to further corruption.

Finally, the “socio-technical systems (STS) perspective provides the overarching meta-framework, asserting that optimal organizational performance is achieved only when the social system (people, culture, skills) and the technical system (tools, infrastructure, processes) are jointly optimized and designed for mutual coherence. This lens is critical for framing the findings on information security and usability. It posits that a failure in the technical subsystem (e.g., a non-integrated database) is intrinsically linked to a failure in the social subsystem (e.g., a lack of data governance culture), and vice versa. A secure, anti-corruption ICT framework, therefore, requires a joint design approach that addresses technology, human factors, and institutional rules as a single, indivisible system. This theoretical synthesis allows the study to frame the barriers to ICT-facilitated anti-corruption not merely as technical or financial deficits but as fundamental failures in designing systems that are trusted, valued, and usable by the end-user, while operating within a supportive institutional environment.

Methodology

This study employs a narrative review methodology, which is particularly appropriate for synthesizing diverse streams of interdisciplinary literature to generate holistic interpretations and novel conceptual frameworks (Hill & Burrows, 2017). This approach is best suited for descriptive and explanatory research where the objective is to integrate findings across multiple studies, guided by the researcher's expertise and existing theoretical models (Bell, 2017; Scarnato, 2017). The narrative methodology facilitates a critical reflection and a comprehensive understanding of the complex, socio-technical problem of ICT and corruption, allowing for the synthesis of technical, social, and policy-oriented research into a coherent set of strategic recommendations.

Data Collection Strategy

A purposive collection of peer-reviewed academic and professional literature was conducted. Searches were performed across the ProQuest databases, Science Direct, and the Walden University library, utilizing keywords such as "e-governance and corruption," "ICT adoption Nigeria," "data governance," "technology acceptance model," and "information security human factors." The review incorporated 38 references, ensuring a rigorous scholarly foundation. Over ninety percent (92%) of the total references are peer-reviewed, and 71% are drawn from peer-reviewed journals published within a five-year window of the study, ensuring both credibility and currency of the synthesized evidence.

Discussion of Findings

The synthesis of literature reveals that a sustainable technology-driven fight against corruption in Nigeria is contingent on a tripartite strategy that goes far beyond mere infrastructure procurement.

Automation and Discretion Elimination

The foundational finding is that technology only mediates corruption effectively when it enforces total automation, thereby removing human discretion. The failure of traffic systems and financial platforms demonstrates that systems allowing for manual override, selective enforcement, or that lack comprehensive backend databases are not merely ineffective but counterproductive. They create new rent-seeking opportunities for those who control the "off switch" or interpret the loopholes. Effective ICT must function as a closed-loop, end-to-end system where data capture, verification, and consequence are automated and non-negotiable.

Data and E-Governance as a Deterrence Mechanism

The efficacy of e-governance as a corruption deterrent is dependent on a robust data governance framework that ensures a single, verifiable source of truth (Bennett, 2017; Khatri & Brown, 2010). The discussion reveals that Nigeria’s fragmented data landscape prevents the cross-referencing that is essential for detecting and proving illicit enrichment and conflict of interest. A functional anti-corruption framework must integrate databases across agenciesfrom vehicle registration and tax records to land registries and public procurementmaking assets and transactions visible. Furthermore, the systematic publication of data on public expenditure and the identities of corrupt culprits (deterrence) can only be effective when this data is considered trustworthy by the public, a trust born from a demonstrably secure and accurate system.

The Primacy of the Human Factor and Usability in Security

Finally, the study confirms that technology is not a panacea, as humans remain the most critical vulnerability in any information security system (Stallings & Brown, 2012; Komatsu*et al.,* 2013). However, this discussion extends the human factor beyond mere "insider threats" to include the system design’s failure to account for Nigeria's socio-cultural context. A secure, anti-

corruption ICT system must be a "usable secure system." The staggering rates of cash-based transactions and the digital divide are not simply "user problems" to be solved by training; they are symptoms of a profound design failure to account for Perceived Ease of Use and to build trust. The findings suggest that an interface that accommodates low literacy, offers multilingual support, and provides transparent, unalterable records of transactions can build user confidence and significantly widen the net of citizen participation in a transparent digital economy, simultaneously shrinking the informal, cash-based spaces where corruption thrives.

Conclusion and Recommendations

In conclusion, the path to a corruption-free future through technology is not through the quantity of ICT investment, but through the quality of its strategic integration into the socio-technical fabric of governance. It requires a deliberate shift from viewing ICT as a threat to be neutralized, to leveraging it as a trusted, accessible, and secure ecosystem. This transition holds the potential to catalyze profound social change, enhancing institutional integrity and empowering Nigerian citizens to be the ultimate guardians of accountability.

This study concludes that the eradication of corruption through ICT in Nigeria is not a task of simple technological procurement but a complex project of institutional and cultural transformation. The core objective is to deploy ICT as a framework that is automated, transparent, and accountable. Based on the synthesized findings, the following policy and implementation recommendations are proposed:

i. The government must prioritize the development of integrated, national-scale databases with real-time inter-agency operability, particularly in high-risk sectors such as customs, procurement, traffic management, and public finance. Automation must be absolute, eliminating manual intervention and bureaucratic discretion at critical points of service delivery and enforcement.

ii. ICT adoption strategies must undergo a paradigm shift to accommodate the country's literacy levels and cultural diversity. This requires the development of user interfaces that are icon-driven, voice-activated, and multilingual, as a means to build trust and operationalize TAM's Perceived Ease of Use. Without this focus, e-governance will remain an elitist tool, alienating the majority of citizens and perpetuating the digital divide.

iii. A comprehensive, mandatory information security culture must be cultivated across all public sector ICT deployments. This framework must integrate stringent policies (principles, rules, and guidelines) and continuous behavioral training that addresses the psychology of security breaches, ensuring that the "human link" transforms from the weakest point to a resilient line of defense.

iv. The dual implementation of robust data governance and open data initiatives is critical. By ensuring data integrity and systematically publishing anonymized procurement data and lists of sanctioned corrupt entities, the state can deploy "transparency as deterrence," leveraging

ICT to not just catch but to discourage corrupt acts by increasing the perceived risk of exposure.

References

Bennett, S. (2017). What is information governance and how does it differ from data governance? Governance Directions, 69(8), 462-467.

Chen, S., Liu, S., Li, S., & Yen, D. C. (2013). Understanding the mediating effects of relationship

quality on technology acceptance: An empirical study of e-appointment system. Journal of Medical Systems, 37(6), 9981.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

Emengini, S. E., &Alio, F. C. (2014). Cashless economy and financial statement reporting in Nigeria. European Center for Research Training and Development, 2(3), 1-9

.Fenz, S., Heurix, J., Neubauer, T., &Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410-430.

Güney, T. (2017). Governance and sustainable development: How effective is governance? *The Journal of International Trade & Economic Development, 26(3), 316-335.

Ionescu, L. (2013). The impact that e-government can have on reducing corruption and enhancing transparency. Economics, Management, and Financial Markets, 8(1), 210-215.

Itah, A. J., &Ene, E. E. (2014). Impact of cashless banking on banks' profitability. *Asian Journal of Finance & Accounting, 6, 362-376.

Kaushik, A. K., & Rahman, Z. (2015). Innovation adoption across self-service banking technologies in India. The International Journal of Bank Marketing, 33(2), 96-121.

Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152.

Koltay, T. (2016). Data governance, data literacy and the management of data quality. International Federation of Library Associations and Institutions, 42(4), 303-312.

Komatsu, A., Takagi, D., &Takemura, T. (2013). Human aspects of information security. Information Management & Computer Security, 21(1), 5-15.

Krishnan, S., Teo, T. S. H., & Lim, V. K. G. (2013). Examining the relationships among e-government maturity, corruption, economic prosperity and environmental degradation: A cross-country analysis. Information & Management, 50(8), 638-649.

Ogutu, S. O., Okello, L. J., & Otieno, D. J. (2014). Impact of Information and Communication Technology-based market information services on smallholder farm input use and productivity: The case of Kenya. World Development, 64, 311-321.

Sahi, G. K., & Gupta, S. (2013). Predicting customers' behavioral intentions toward ATM services. Journal of Indian Business Research, 5(4), 251-270.

Scott, W. R. (2014). Institutions and organizations: Ideas, interests, and identities(4th ed.). Sage.

Stallings, W., & Brown, L. (2012). Computer security: Principles and practice (2nd ed.). Prentice Hall.

Teoh, W. M., Siong, C. C., Lin, B., &Jiat, W. C. (2013). Factors affecting consumers' perception of electronic payment: An empirical analysis. Internet Research, 23(4), 465-485.

Transparency International. (2020). Corruption Perceptions Index 2019. Retrieved from http://www.transparency.org/policy_research/surveys_indices/cpi/2019

Tsai, H. S. (2015). Understanding the model of senior citizens' mobile-technology acceptance. International Journal of Human-Computer Interaction, 31(4), 277-290.

UNESCO. (2015). Global education monitoring report 2015: Education for all 2000-2015: Achievements and challenges. United Nations Educational, Scientific and Cultural Organization.

Wickberg, S. (2013). Technological innovations to identify and reduce corruption. U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute.