CONFERENCE PROCEEDINGS

October 31-November 2, 2025

Seattle, USA

GLOBAL CONFERENCE ALLIANCE INC. ™

www.globalconference.ca

Proudly American, Truly Global

Conference Proceeding

October 31-November 2, 2025 Seattle, USA

Format: Electronic Book

ISBN: 978-1-997875-10-9

Address
300 Lenora Street #1497,
Seattle, WA 98121, United States

+1 672-971-2088 (Hotline)
Mon to Fri (10 am – 6 pm PST)

Global Conference Alliance Inc.
contact@globalconference.ca

Table of Contents

Content Details:

Jane Wambui Kuria(Author) *Mount Kenya University*	**Exploring the Role of Mobile Money in Advancing Financial Inclusion within 3–5 Star Hotels in Nairobi, Kenya: Trends, Opportunities, and Operational Barriers**

Abstract

The proliferation of mobile money services has significantly reshaped financial landscapes across sub-Saharan Africa, offering novel pathways toward enhanced financial inclusion (DemirgüçKunt et al., 2018). In Kenya, platforms such as M-Pesa have been pivotal in bridging gaps in access to financial services, particularly within sectors traditionally reliant on cash-based transactions. This study investigates the role of mobile money in advancing financial inclusion among 3–5 star hotels in Nairobi, Kenya, with particular emphasis on adoption trends, emerging opportunities, and operational barriers. Drawing on the Technology Acceptance Model (TAM) (Davis, 1989) and Financial Inclusion Theory (Sarma, 2008), the research examines how perceptions of usefulness and ease of use shape the uptake of mobile money technologies and how these systems contribute to expanding financial access within the hospitality industry. Employing a mixed-methods research design, the study integrates quantitative survey data with qualitative insights from hotel managers to offer a nuanced understanding of mobile money integration. Initial findings suggest that mobile money adoption has streamlined payment processes, improved liquidity management, and expanded the client base by offering more flexible payment options. Nevertheless, the research identifies persistent challenges, including cybersecurity vulnerabilities, system interoperability issues, regulatory compliance burdens, and operational disruptions, which collectively constrain the full realization of mobile money's potential in the hotel sector. The study contributes to the growing body of literature on digital financial services by illustrating the dual role of mobile money as both a technological innovation and a financial inclusion mechanism within an urban hospitality context. The findings offer actionable insights for hotel operators, mobile service providers, and policymakers seeking to harness digital payment platforms to foster greater operational resilience and inclusive economic growth.

Keywords: *Mobile Money; Financial Inclusion; Technology Acceptance Model; Hospitality Industry; 3–5 Star Hotels; Nairobi; Digital Financial Services; Operational Barriers*

1.0 Introduction

Financial inclusion has emerged as a cornerstone of sustainable economic development, underpinning efforts to reduce poverty, promote equitable growth, and enhance the resilience of underserved populations. The World Bank (2022) estimates that over 1.4 billion adults globally remain unbanked, with Sub-Saharan Africa bearing a disproportionate share of this financial exclusion. In response, digital financial services particularly mobile money has gained global recognition as effective tools for expanding access to financial systems, especially in regions where traditional banking infrastructure is limited or inaccessible (World Bank, 2022; GSMA, 2021).

East Africa has positioned itself as a global leader in mobile money adoption, with Kenya often cited as a model for mobile financial innovation. Platforms such as M-Pesa have revolutionized the way individuals and businesses engage in financial transactions, contributing significantly to financial inclusion across multiple sectors (Jack & Suri, 2014). The Kenyan government, through its Vision 2030 development blueprint, has explicitly recognized the role of mobile and digital technologies in fostering inclusive economic growth and improving service delivery across industries, including tourism and hospitality (Government of Kenya, 2018).

Mobile money usage in Kenya has become deeply embedded in everyday economic life. While much of the existing research has focused on the impact of mobile money on low-income households, micro-enterprises, and informal economies, less attention has been paid to its adoption within formal business environments such as the hospitality industry. This sector, particularly 3– 5 star hotels in urban centers like Nairobi, plays a vital role in Kenya's economy—contributing to employment, foreign exchange earnings, and national GDP. The study titled *Exploring the Role of Mobile Money in Advancing Financial Inclusion within 3–5 Star Hotels in Nairobi, Kenya: Trends, Opportunities, and Operational Barriers* addresses this gap by examining how mobile money is being integrated into hotel operations, what opportunities it presents for financial inclusion, and the operational challenges encountered in the process.

Despite the rapid growth of mobile money services in Kenya, research has largely focused on their impact within informal economies, rural communities, and micro-enterprises, leaving a significant knowledge gap regarding their integration into formal business sectors such as the hospitality industry. Specifically, while mobile money platforms like M-Pesa have become ubiquitous in everyday transactions, the extent to which 3–5 star hotels in Nairobi have adopted these technologies—and the resulting implications for financial inclusion—remains underexplored. This gap is critical given the role of the hospitality sector as a major contributor to Kenya's GDP, employment, and international competitiveness (Government of Kenya, 2018).

Furthermore, understanding the adoption and operational challenges of mobile money in upscale hotels is increasingly important as consumer expectations shift toward cashless and digital payment options, particularly in the aftermath of the COVID-19 pandemic (World Bank, 2022). Hotels that fail to adapt to these technological trends risk alienating a growing segment of digitallysavvy customers and may struggle to optimize operational efficiency and financial transparency. At the same time, the integration of mobile money services within formal hospitality settings raises complex operational, regulatory, and cybersecurity concerns. Without a clear understanding of these barriers and the opportunities mobile money presents, both hotel operators and policymakers may miss crucial avenues for advancing digital financial inclusion within one of the most visible and economically significant sectors of the Kenyan economy.

By investigating mobile money usage within this underexplored context, the study contributes to a more holistic understanding of digital financial inclusion. It highlights key trends such as increased adoption of mobile payments for reservations and service transactions, emerging opportunities for enhanced guest convenience and revenue tracking, and persistent barriers including regulatory compliance, interoperability issues, and cybersecurity risks. These findings are critical not only for stakeholders in Kenya's hospitality sector but also for broader policy and industry efforts aimed at strengthening the role of mobile money in driving inclusive and resilient economic development.

This research is therefore essential in filling a critical gap in the literature by systematically exploring trends, opportunities, and operational barriers associated with mobile money usage in Nairobi's 3–5-star hotel industry. The findings are expected to inform hotel management practices, guide policymakers in creating enabling regulatory environments, and contribute to the broader discourse on digital financial inclusion strategies in developing economies.

1.1 Research Objective and Contribution

The primary objective of this study is to critically examine how mobile money adoption advances financial inclusion within 3–5 Star hotels in Nairobi, Kenya, by identifying prevailing trends, emerging opportunities, and operational barriers associated with its use in the hospitality sector. This research contributes to the growing body of knowledge on digital financial inclusion by extending analysis beyond informal and rural contexts to a formal, urban service industry critical to Kenya's economy. By focusing on 3–5 star hotels—an often overlooked sector in mobile money research—the study provides new empirical insights into how digital financial technologies are reshaping service delivery, financial practices, and customer engagement in the hospitality industry. Furthermore, the findings offer actionable recommendations for hotel operators, policymakers, and financial service providers seeking to optimize mobile money integration, thus promoting greater economic inclusion, operational resilience, and technological advancement within Kenya's digital economy

2.0 Literature Review 2.1 Mobile Money and Financial Inclusion

Mobile money has been globally recognized as a transformative tool for enhancing financial inclusion, particularly in developing economies where traditional banking infrastructure remains limited. According to the World Bank (2022), digital financial services, including mobile money, have significantly expanded access to financial systems, allowing underserved populations to engage in saving, borrowing, and secure transactions. GSMA (2021) further emphasizes that SubSaharan Africa accounts for nearly half of all mobile money accounts worldwide, with services like M-Pesa in Kenya leading the movement.

Research by Jack and Suri (2014) demonstrated that mobile money services not only facilitate everyday transactions but also contribute to poverty reduction and risk mitigation among users. Subsequent studies have reinforced these findings, highlighting how mobile financial services lower transaction costs, increase financial resilience, and open new economic opportunities for individuals and businesses (Demirgüç-Kunt et al., 2018). However, most literature focuses on lowincome households, rural settings, or micro-enterprises, leaving a research gap concerning the integration of mobile money within formal, urban industries such as hospitality.

2.2 Mobile Money Adoption in Business Sectors

While early research predominantly addressed individual-level adoption, recent studies have explored how businesses leverage mobile money to improve operational efficiency, enhance customer experience, and secure revenue streams. Munyegera and Matsumoto (2018) found that mobile money use among small and medium enterprises (SMEs) led to increased sales volumes and improved financial management practices. In the Kenyan context, Gikandi and Bloor (2010) noted that businesses adopting mobile payment platforms experienced greater financial transparency and expanded their customer base.

Despite these advantages, businesses also face significant challenges related to mobile money adoption, including concerns over data security, transaction limits, regulatory compliance, and interoperability between different financial platforms (Kikulwe, Fischer, & Qaim, 2014). These operational barriers are particularly pronounced in sectors requiring high levels of financial accountability and customer service excellence, such as the hospitality industry.

2.3 Mobile Money and the Hospitality Sector

The hospitality industry is a major economic contributor in many emerging markets, yet studies focusing on technological innovations in this sector especially mobile money adoption are limited. According to Law, Leung, and Buhalis (2019), digital payment systems have become essential components of modern hotel management, improving operational efficiency and enhancing guest satisfaction. In Kenya, mobile money's penetration into the hospitality sector is seen as an opportunity to cater to a growing tech-savvy local and international clientele (Kenya Tourism Board, 2020).

Nevertheless, barriers persist. Hotels must navigate cybersecurity risks, ensure seamless integration of mobile money with other financial systems, and train staff adequately to manage new technologies (Adukaite et al., 2017). Moreover, upscale hotels, such as 3–5 star establishments, face unique challenges related to customer expectations for premium service quality and data security, raising questions about the readiness of such institutions to fully embrace mobile money solutions.

2.4 Theoretical Framework

This study was anchored on two key theories: Technology Acceptance Model (TAM) and Financial Inclusion Theory.

2.4.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model was proposed by **Davis (1986; 1989)**. It explains user adoption of technology based on two key constructs: *Perceived Usefulness* (PU) — the degree to which a person believes that using a particular system would enhance their job performance and *Perceived Ease of Use* (PEOU) the degree to which a person believes that using a system would be free from effort. In the context of this study, TAM will be used to understand the acceptance and integration of mobile money technologies by 3–5 star hotels in Nairobi. The model explains how perceived benefits and simplicity of mobile money influence adoption rates within hotel operations.

2.4.2 Financial Inclusion Theory

Financial Inclusion Theory emphasizes that economic growth and poverty reduction are greatly influenced by equitable access to financial services. It highlights that when individuals and businesses (such as hotels) gain access to affordable financial services — savings, payments, insurance, and credit — they are better positioned to participate in economic activities and improve their financial wellbeing. In this study, Financial Inclusion Theory supports the view that mobile money platforms facilitate financial inclusion for hotels by simplifying transactions, promoting customer reach, and reducing operational barriers traditionally associated with banking. **2.5 Research Gap**

Although existing literature acknowledges the transformative impact of mobile money across various sectors, there remains a notable gap regarding its adoption, benefits, and challenges within formal, high-end service industries like 3–5 star hotels in Nairobi. The study *Exploring the Role of Mobile Money in Advancing Financial Inclusion within 3–5 Star Hotels in Nairobi, Kenya: Trends, Opportunities, and Operational Barriers* seeks to address this gap by providing empirical evidence on mobile money's role in advancing financial inclusion in Kenya's premium hospitality sector. This contribution is crucial for broadening the understanding of digital financial ecosystems and informing policy and practice within the formal economy.

2.6 Research Distinctiveness and Contribution to the Field

While extensive research has documented the transformative impact of mobile money on financial inclusion among low-income populations, rural communities, and micro-enterprises (DemirgüçKunt et al., 2018; Jack & Suri, 2014), relatively little attention has been paid to its adoption and operationalization within formal, high-value sectors such as the hospitality industry. Most prior studies have concentrated on informal economic activities or small-scale business operations, often overlooking how mobile money technologies are reshaping formal service industries that cater to both domestic and international clienteles.

This study differs from previous research in several important ways. First, it shifts the focus from informal sectors to the formal, structured environment of 3–5 star hotels in Nairobi, which represent a critical and economically significant part of Kenya's tourism and service economy. By doing so, it addresses a significant gap in the literature and contributes to a more nuanced understanding of how mobile money can drive financial inclusion across different sectors of the economy.

Second, unlike earlier studies that predominantly examine either the benefits or the challenges of mobile money adoption in isolation (Gikandi & Bloor, 2010; Kikulwe, Fischer, & Qaim, 2014), this research adopts a comprehensive approach by concurrently analyzing prevailing trends, emerging opportunities, and operational barriers within the hospitality context. This integrated perspective allows for a more holistic understanding of the dynamics influencing mobile money adoption and its implications for business innovation and customer experience.

Third, by focusing on high-end hotels, the study addresses operational complexities such as heightened cybersecurity demands, regulatory compliance, and client expectations for premium service standards that are typically absent from discussions centered on low-cost, informal, or rural enterprises. These insights are critical for informing sector-specific strategies aimed at fostering digital financial inclusion within sophisticated, service-oriented industries.

Finally, the findings are intended not only to advance theoretical knowledge but also to offer practical recommendations for hotel managers, technology providers, and policymakers. The aim is to optimize the integration of mobile money systems, enhance operational efficiency, and better meet the evolving needs of digitally connected consumers in Kenya's vibrant hospitality market. Through these distinct contributions, the study offers a broader and deeper understanding of the role of mobile money in advancing financial inclusion and digital transformation within the formal economy of emerging markets.

3.0Methodology

This study adopted a mixed-methods research design to comprehensively explore the role of mobile money in advancing financial inclusion within 3–5 star hotels in Nairobi, Kenya. The combination of qualitative and quantitative approaches enabled a nuanced understanding of both the operational realities and strategic perspectives surrounding mobile money adoption in the hospitality sector. A concurrent triangulation design was employed, allowing the collection of both quantitative and qualitative data within the same timeframe. This design facilitated the crossvalidation and integration of findings to ensure a robust analysis of the trends, opportunities, and operational barriers associated with mobile money usage in formal hotel operations.

The study targeted 3–5 star hotels located in Nairobi County, as classified by the Tourism Regulatory Authority (TRA). These hotels were selected due to their strategic role in Kenya's tourism sector and their potential for digital financial integration. A purposive sampling technique was used to identify hotel managers, finance officers, front office supervisors, and IT staff as key informants due to their direct involvement with financial and technological systems. Quantitative data were collected from a sample of 25 hotels, using structured questionnaires administered to a total of 100 respondents. The sample was designed to capture diversity in hotel size, ownership (local vs. international), and customer base.

Quantitative data were collected using a structured questionnaire consisting of closed-ended items designed to assess mobile money adoption rates, transaction volumes, integration with other systems, and perceived benefits. The questionnaire was pilot-tested with 10 respondents to ensure clarity and reliability.

Qualitative data were obtained through semi-structured interviews conducted with 15 key hotel personnel. The interview guide covered topics such as operational challenges, customer preferences, regulatory concerns, and future strategies related to mobile money. All interviews were audio-recorded (with participant consent), transcribed verbatim, and thematically coded. Quantitative data were analyzed using descriptive statistics (frequencies, means, standard deviations) and inferential statistics (correlation analysis) using SPSS software. This helped identify patterns and relationships between variables such as hotel category, level of mobile money integration, and perceived customer satisfaction.

Qualitative data were analyzed thematically using NVivo software. Coding was both deductive (based on the research questions) and inductive (emerging from the data), allowing for a detailed exploration of perceived opportunities and barriers.

3.1 Ethical Considerations

Ethical approval was obtained from the relevant institutional review board prior to data collection. Participants were informed about the purpose of the study, assured of confidentiality, and provided written consent. All data were anonymized and stored securely to protect participant identity.

4.0 Results

This section presents the quantitative and qualitative findings from the study on mobile money adoption and financial inclusion in 3–5 Star hotels in Nairobi, Kenya. The results are organized around the three core areas of investigation: trends, opportunities, and operational barriers.

4..1 Mobile Money Adoption Trends

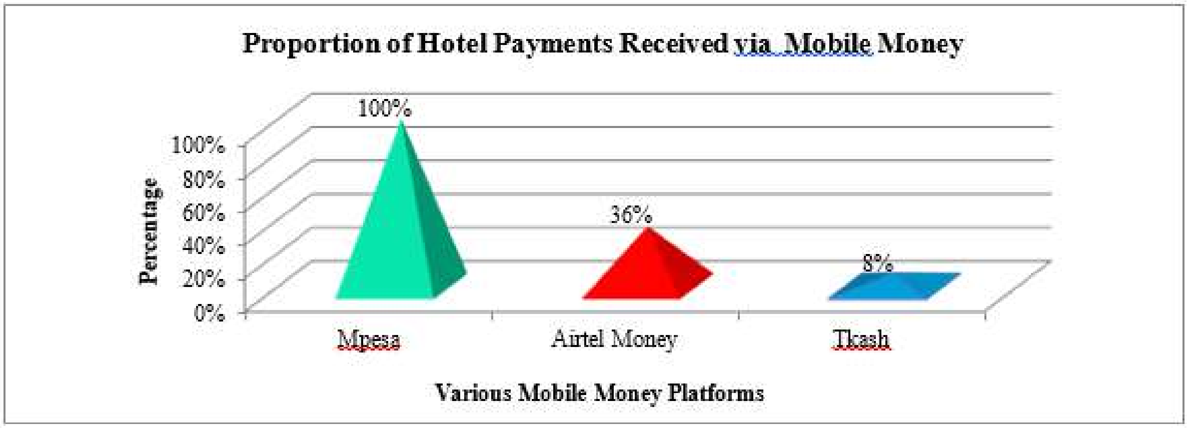
Out of the 25 participating hotels, 92% (n = 23) reported accepting mobile money payments from guests, with M-Pesa cited as the most widely used platform (100% of adopters), followed by Airtel Money (36%) and T-Kash (8%). Table 1 summarizes the prevalence of mobile money platforms across the surveyed hotels.

Table 1: Adoption of Mobile Money Platforms in among 3-5-star rates hotels

Mobile Money Platform	Adoption Rate (%)
M-Pesa	100%
Airtel Money	36%
Mobile Money Platform	**Adoption Rate (%)**
T-Kash	8%

In terms of transaction volumes, 68% of the hotels indicated that mobile money accounted for between 30% and 50% of all customer payments, suggesting a strong but partial shift toward digital transactions (Figure 1).

Figure 1: **Proportion of Hotel Payments Received via Various Mobile Money**



(actual bar chart.)

4.2 Perceived Opportunities of Mobile Money

Survey respondents ranked various benefits of mobile money on a Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). Table 2 presents the mean ratings.

Table 2: **Perceived Benefits of Mobile Money Integration**

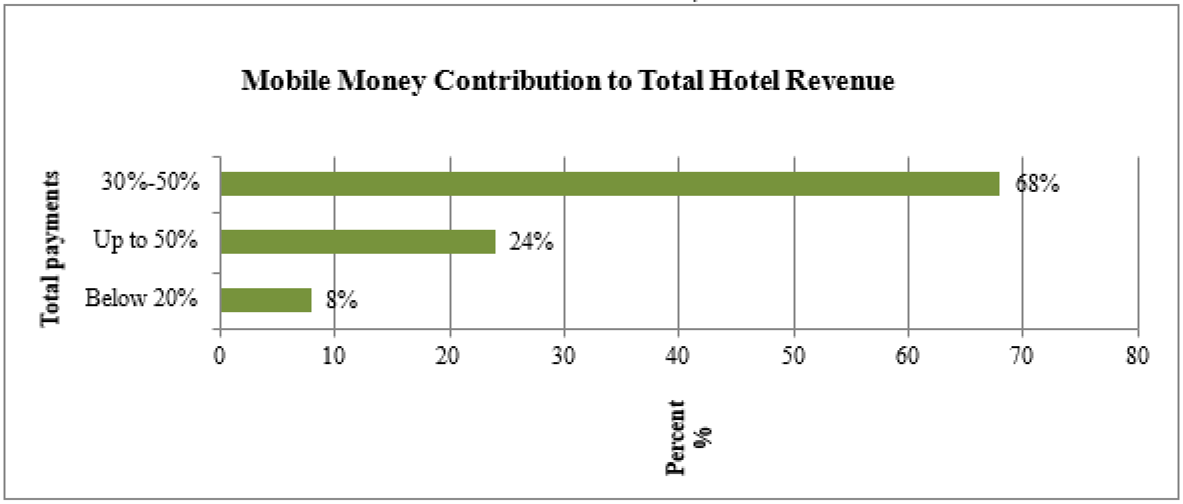
Opportunity	Mean Score (M)	Standard Deviation (SD)
Faster transaction processing	4.56	0.61
Greater financial transparency	4.28	0.75
Increased customer satisfaction	4.15	0.68
Reduction in cash handling risks	4.02	0.79
Easier financial reconciliation	4.00	0.73

Faster payment processing received the highest mean score (M = 4.56, SD = 0.61).

4.3 Contribution of Mobile Money to Hotel Revenue

68% of hotels indicated that mobile money transactions accounted for between 30% and 50% of their total customer payments, while 24% reported mobile money making up over 50% of transactions. Only 8% indicated less than 20% contribution.

Figure 2: **Mobile Money Contribution to Total Hotel Revenue**



(*Bar chart: 68% = 30–50%; 24% = >50%; 8% = <20%*)

4.4 Operational Barriers to Mobile Money Utilization

The main challenges cited included high transaction fees (72% of respondents), cybersecurity concerns (64%), and system integration difficulties with existing hotel management software (48%), Staff training and adaptation challenges (32%).

Table 3: **Operational Barriers Identified**

Barrier	**Percentage Reporting (%)**
High transaction costs	72%
Cybersecurity vulnerabilities	64%
Difficulty integrating with PMS systems	48%
Staff training issues	32%

4.5 Increasing Customer Expectations for Digital Payments

Participants consistently noted that local and international guests increasingly prefer mobile money options, expecting fast, contactless transactions.

"Many of our customers, especially younger ones, ask if they can pay everything — even room service — using M-Pesa." (Front Office Manager, 5-star hotel)

4.6 Operational Challenges and Costs

Respondents cited issues such as frequent system downtimes, reconciliation errors, and perceived high commissions charged by mobile money operators.

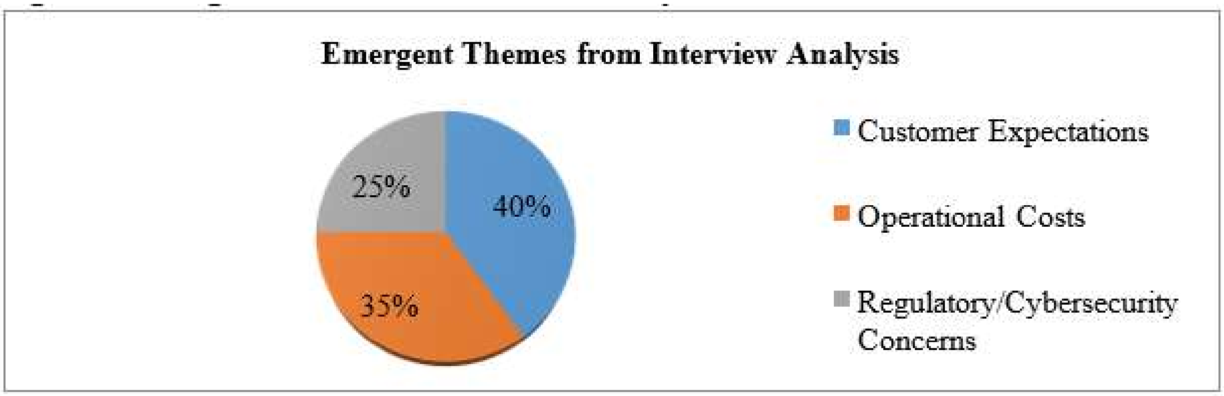
"Integration with our existing billing system was expensive and needed custom solutions." (Finance Manager, 4-star hotel)

4.7 Need for Stronger Regulatory and Cybersecurity Frameworks

Participants emphasized the need for clearer regulations to protect customer data and mitigate risks of fraud when handling high-value transactions.

"We sometimes feel exposed to fraud risks, especially for big transactions, yet there's little legal recourse if things go wrong." (Hotel IT Officer, 5-star hotel)

Figure 3: **Emergent Themes from Interview Analysis**



(*Pie chart showing: Customer expectations – 40%, Operational costs – 35%, Regulatory/cybersecurity concerns – 25%*)

4.8 Summary of Results

The findings demonstrate widespread adoption of mobile money in Nairobi's 3–5 star hotels, driven by customer demand and operational benefits. However, significant operational and regulatory challenges persist, posing potential barriers to fully leveraging mobile money for enhanced financial inclusion within the sector.

5.0 Discussion & Summary

The results of this study provide important insights into the role of mobile money in advancing financial inclusion within Nairobi's 3–5 star hotels. Overall, the findings align with global and regional trends emphasizing the growing dominance of digital payment ecosystems (Demirgüç-Kunt et al., 2018; World Bank, 2022), yet also highlight sector-specific opportunities and persistent operational challenges.

The near-universal adoption of M-Pesa among surveyed hotels confirms the platform's continued market dominance in Kenya's digital financial services landscape (Jack & Suri, 2014). The finding that mobile money transactions constitute between 30% and 50% of total customer payments for the majority of hotels indicates significant customer reliance on mobile money even within the premium hospitality sector, traditionally associated with card and cash transactions. This trend reflects a broader shift in consumer behavior toward cashless, mobile-driven financial interactions, consistent with regional reports on East Africa's financial digitalization (GSMA, 2022).

The study reveals that mobile money integration delivers substantial operational benefits to hotels, particularly in terms of faster transaction processing, enhanced transparency, and reduced cashhandling risks. These findings resonate with earlier research by Gikandi and Bloor (2010), which demonstrated that mobile payment systems improve business process efficiencies. The relatively high mean scores for customer satisfaction (M = 4.15) suggest that mobile money contributes to an enhanced service experience, positioning hotels that embrace digital payments competitively within the increasingly tech-savvy tourism market.

Despite the clear benefits, the findings highlight significant operational barriers that could undermine the full potential of mobile money in this sector. The high cost of transactions, reported by 72% of hotels, mirrors concerns raised by Kikulwe, Fischer, and Qaim (2014) regarding the affordability of mobile money services for businesses. Furthermore, cybersecurity concerns, cited by 64% of respondents, are particularly pertinent in the context of high-value hotel transactions, which differ markedly from the lower-value transactions typically emphasized in mobile money literature.

The challenges surrounding system integration with hotel management software (reported by 48%) suggest that digital transformation in the hospitality industry requires more tailored technological solutions than those available for informal retail or rural markets. This supports calls by contemporary scholars for sector-specific financial technology innovations to support formal enterprises (Ozili, 2018).

Unlike prior studies focused predominantly on informal sectors or low-income users (Aker & Mbiti, 2010), this research demonstrates that mobile money has penetrated even formal, internationally oriented industries like hospitality. Moreover, the emerging need for enhanced regulatory frameworks and cybersecurity measures distinguishes the operational environment of 3–5 star hotels from that of small businesses, highlighting the unique challenges faced by larger, formal organizations.

5.1 Conclusion

This study contributes to the literature by shifting the focus from informal economies to formal service industries and by presenting an integrated view of both opportunities and barriers. The findings underscore the importance of designing mobile money solutions that address the complexities of enterprise-level operations while promoting financial inclusion across different economic strata.

5.2 Recommendations

One limitation of this study is its focus on hotels within Nairobi only, which may not reflect the realities of hotels in other parts of Kenya or East Africa. Additionally, the study relied on selfreported data, which could be subject to reporting bias. Future research could explore longitudinal impacts of mobile money adoption in hotels, assess guest satisfaction quantitatively, and examine the effectiveness of mobile money-related cybersecurity interventions in the hospitality industry.

References

Adukaite, A., von Zyl, I., Er, Ş., & Cantoni, L. (2017). Technology-enhanced tourism education: A case study of South African hotels. *Education and Information Technologies*, 22(4), 1465–1481. https://doi.org/10.1007/s10639-016-9503-0

Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa. *Journal of Economic Perspectives, 24*(3), 207–232. https://doi.org/10.1257/jep.24.3.207 SSRN+3Taylor & Francis Online+3American Economic Association+3

Allen, F., Demirgüç-Kunt, A., Klapper, L., & Pería, M. S. M. (2016). The foundations of financial inclusion: Understanding ownership and use of formal accounts. *Journal of Financial Intermediation*, 27, 1–30.

Davis, F. D. (1986). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*. (Doctoral dissertation, Massachusetts Institute of Technology).

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

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*. World Bank. https://doi.org/10.1596/978-1-4648-1259-0

Gikandi, J. W., & Bloor, C. (2010). Adoption and effectiveness of electronic banking in Kenya. *Electronic Commerce Research and Applications*, 9(4), 277–282. https://doi.org/10.1016/j.elerap.2010.05.001

Government of Kenya. (2018). *Kenya Vision 2030: The popular version*. Government Printer

GSMA. (2022). *The state of the industry report on mobile money 2022*. https://www.gsma.com/sotir/wp-content/uploads/2024/03/GSMA-SOTIR 2024_Report.pdfGSMA.

GSMA. (2021). *State of the industry report on mobile money 2021*. GSMA. https://www.gsma.com/sotir/

Jack, W., & Suri, T. (2014). Risk sharing and transactions costs: Evidence from Kenya's mobile money revolution. *American Economic Review*, 104(1), 183–223. https://doi.org/10.1257/aer.104.1.183

Jack, W., & Suri, T. (2011). Mobile money: The economics of M-PESA. *National Bureau of Economic Research Working Paper No. 16721*. https://doi.org/10.3386/w16721NBER Kenya Tourism Board. (2020). *Annual Tourism Sector Performance Report 2019/2020*. Kenya Tourism Board.

Kikulwe, E. M., Fischer, E., & Qaim, M. (2014). Mobile money, smallholder farmers, and household welfare in Kenya. *PLoS ONE*, 9(10), e109804. https://doi.org/10.1371/journal.pone.0109804

Law, R., Leung, R., & Buhalis, D. (2019). Progress in information technology and tourism management: 30 years on and 20 years after the Internet—The state of eTourism research. *Tourism Management*, 69, 460–470. https://doi.org/10.1016/j.tourman.2018.06.002 Munyegera, G. K., & Matsumoto, T. (2018). ICT for financial access: Mobile money and the financial behavior of rural households in Uganda. *Review of Development Economics*, 22(1), 45–66. https://doi.org/10.1111/rode.12308

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review, 18*(4), 329–340. https://doi.org/10.1016/j.bir.2017.12.003Taylor & Francis Online+1SCIRP+1

Sarma, M. (2008). Index of Financial Inclusion. *Indian Council for Research on International Economic Relations (ICRIER)*, Working Paper No. 215.

World Bank. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank. https://doi.org/10.1596/978-1-4648-1897-4

World Bank. (2022). *Mobile money and the economy: A review of evidence*. https://openknowledge.worldbank.org/handle/10986/31280 Open Knowledge Bank+1 OUPAcademic+1

Pabitra Mandal
Roskilde University

How Digital Transformation and Cybersecurity Issues Affect Business Resilience?

Abstract

Digital transformation has become a critical strategic priority for organizations across industries, driven by the need for efficiency, agility, and innovation in an increasingly interconnected world. The COVID-19 pandemic further accelerated this shift, compelling enterprises to adopt technologies such as artificial intelligence (AI), Internet of Things (IoT), blockchain, and cloud computing. While these technologies offer substantial operational benefits, they also expose organizations to sophisticated cybersecurity threats that can compromise sensitive data, disrupt services, and damage stakeholder trust. This paper explores the complex interplay between digital transformation and cybersecurity, with a particular focus on how these dynamics influence business resilience. This research highlights both the transformative potential of digital tools and the vulnerabilities they introduce. Key challenges identified include data breaches, ransomware, identity theft, lack of skilled cybersecurity professionals, regulatory gaps, and low digital literacy among employees. Special attention is given to sector-specific insights, such as financial institutions' struggles with fraud and customer trust, healthcare systems' privacy and device security concerns, and governments' need to secure digital public infrastructure.

1. Introduction:

Digital transformation means using digital tools and technologies in how businesses operate. This can lead to major changes in different parts of a company, such as how they deal with customers, how they manage internal processes, who their target market is, and even the company's culture. During the COVID-19 pandemic, many companies quickly adopted digital tools, which also brought some sudden challenges [1].

Technologies like artificial intelligence (AI), big data, blockchain, cloud computing, the Internet of Things (IoT), and industrial IoT are key to driving digital transformation. While these technologies offer many benefits and have encouraged companies to speed up their digital transformation, they also introduce new cybersecurity risks. To keep their businesses running safely, companies must protect their digital tools and systems from cyber threats [2,3].

Hackers can exploit weaknesses in digital systems. To stop this, companies should use encryption, authentication, and access control to protect data and prevent unauthorized access. They should also consider getting cyber insurance, which helps cover financial losses in case of a cyber-attack. It's also important to train employees so they understand how to stay safe online, because better awareness leads to better security practices [4,5].

Cyber-attacks are increasing and can cause serious problems like stealing sensitive data, demanding money (ransomware), or stopping business operations. So, companies need to understand these threats and take proper steps to protect themselves. Cybersecurity involves defending computers and networks from being hacked or damaged.

The cost of cybersecurity and the damage from cybercrimes are both rising globally [6]. Research by Haislip et al. [7] shows that the total financial impact of cyber-attacks is often underestimated because it affects not just one company but the whole industry, including things like lower stock prices and higher insurance costs.

Garg [8] listed seven key reasons why companies should invest in cybersecurity:

a) Protecting intellectual property
b) Meeting customer needs better
c) Keeping customers from leaving
d) Building trust in secure products
e) Being part of safe networks with other companies
f) Maintaining a good reputation
g) Reducing damage across the industry

Lee [9] introduced a risk management model to help companies improve their cybersecurity over time and make smart investment decisions. Although many companies use the NIST Cybersecurity Framework, it doesn't include cost–benefit analysis. The Gordon–Loeb model helps identify which level of the NIST framework is most cost-effective for a company [10]. Krutilla et al. [11] improved this model by considering that cybersecurity tools lose value over time, which affects how cost-effective they are.

Simon and Omar [12] explained that even if a company is secure, it can still be hurt if a supplier or partner gets hacked. So, cybersecurity planning must also think about risks from connected companies. Uddin et al. [13] found that weak cybersecurity can hurt a company's performance, especially in banking, where online risks are growing. Curti et al. [14] noted that governments are also seeing more cyber-attacks, which is leading to higher spending on cybersecurity and rising overall government costs.

2. Financial Sector

The financial industry is very important for any economy, and many research studies have been done in different regions. For example, Al-Alawi and Al-Bassam did a study in Bahrain and found that financial organizations face threats like identity theft, damage to computer systems, and hacking, which disrupt operations [16]. Similarly, Hasan and Al-Ramadan [17] studied bank customers in Iraq and found that even though banks use strong security measures, some customers still don't fully trust online banking.

Joveda et al. [18] researched the banking sector in Bangladesh. They focused on creating a cybersecurity system to detect money laundering, which harms economic growth. Almudaires and Almaiah [19] talked about the main risks credit card companies face and gave suggestions to improve their cybersecurity. Smith and Dhillon [20] pointed out that blockchain technology can reduce security problems in financial transactions, but more serious analysis is needed before fully using it in this sector.

Kuzmenko et al. [21] used machine learning to study large financial datasets to catch threats early. Rodrigues et al. [22] built a model to help banks bring in AI, digital technologies, and cybersecurity without risking data safety. They found that banks are under pressure to adopt new technologies while also keeping their data safe. They used expert discussions and methods like cognitive mapping and DEMATEL to find key factors affecting AI use in banks, such as customer trust, laws, and availability of skilled workers.

Fedorov et al. [23] talked about using smart technologies to make sure biometric identification (like fingerprints) is secure in online banking. Their study focused on Russia and showed that advanced tech needs strong security to keep customer data safe.

Patil and Bharath [24] studied how new technologies are changing the financial sector. They found that Fintech has helped businesses and increased investor trust, but there are still problems like fraud and low performance. Their study included around 160 people.

Rãƒdulescu et al. [25] pointed out the risks of digitalization, like how it can increase cyber-attacks. They said it’s important to involve tech experts to help manage these growing risks. They also suggested that risk managers should plan well and choose the best security methods. Finally, they emphasized the need for global cooperation to fight cybercrime and highlighted the role of digital tools in business, human interaction, and governance.

3. Health Sector

Cybersecurity in healthcare deals with protecting patient data [26] and keeping medical devices secure [27,28,29,30]. If digital transformation is done safely, it can improve how health organizations are managed [31,32,33].

Garcia-Perez et al. [34] analyzed data from UK healthcare leaders during COVID-19. They found that a strong foundation in cybersecurity knowledge, handling uncertainty, and understanding how different parts of healthcare are connected is important for building digital resilience and sustainable practices.

Paul et al. [35] discussed how digital tools are changing healthcare. They looked at privacy and security issues, the impact on patient care, and new business opportunities through technologies like Industry 4.0. The rise in chronic illness and the pandemic has pushed for more personal healthcare. Digital tools like biosensors are now used for on-demand health services. Big data helps doctors make better decisions while keeping patient information safe.

They listed ways to solve security problems, such as using mutual authentication, blockchain, lightweight cryptography, and more. They also suggested managing medical equipment better and studying how patient involvement affects security. More research is needed on healthcare privacy laws, the use of AI and blockchain, and cloud technology for better data storage and sharing.

Nwaiwu and Mbelu [36] said the GDPR law is important for tracking health, developing businesses, and finding market opportunities. Europe had over 1.9 million COVID-19 cases, and personal data tracking helped control the virus.

Maleh and Mellal [37] wrote about how COVID-19 accelerated digital transformation and also increased cyber-attacks. They grouped challenges into three categories: staying strong against attackers, recovering secure systems, and adapting to new tech needs.

4. Governmental Sector

Many governments, like those in Bahrain [38], the UK [39], and Saudi Arabia [40], have started using digital tools, but not at the same speed. Al Shobaki et al. [41] studied the Ministry of Interior in Palestine and found a strong connection between digital transformation and good cybersecurity. Some key organizational factors like data sharing between departments played a big role in keeping systems secure. In Gaza, the digital impact on cybersecurity was very high (coefficient 0.897).

Al Najjar et al. [42] also studied the same ministry in Palestine. They used surveys and found that digital transformation was mostly in place, but improvements were needed in areas like funding and innovation. They found strong support from management and technical systems but weaker coordination in human resources.

Fjord and Schmidt [43] looked at using digital tools to make tax systems more efficient. Denmark made progress, but cybersecurity and legal safeguards were still needed. Mijwil et al. [44] emphasized the need for strong cybersecurity governance during digital transformation of public services. They recommended strategies to keep services secure and avoid data tampering.

Maglaras et al. [45] focused on protecting national infrastructure from serious cyber-attacks. They suggested a new method for evaluating threats using advanced techniques like fileless attacks.

5. Business Sector

Businesses use different technologies, and modern tools like the Internet of Everything can improve security [46]. Gonchar [47] gave advice for improving economic security using digital tools in Ukraine. They found that many companies use digital tools, but results differ based on size and industry. A method was proposed to measure digital progress, but without staff engagement, benefits were limited. Businesses need more employee training to truly improve performance.

Kuzior et al. [48] looked at how different countries adopt digital tools. They built a model showing how factors like cybersecurity and anti-money laundering laws affect digital growth. Putri et al. [49] showed how Indonesia moved from paper to digital systems. They encouraged public use and suggested evaluating government services using cyber frameworks.

Shitta-Bey [50] explored how cloud computing affects business change. Moving to cloud systems brings risks like data breaches and system weaknesses. The study listed 18 risks in cloud migration and emphasized the need for monitoring and security plans.

Trung et al. [51] studied AI, blockchain, and IoT in e-commerce. They found these tools increase security and efficiency, but high costs and complexity are barriers. Gul et al. [52] studied ecommerce in Saudi Arabia and found that customers don't fully trust these sites due to weak security. Saeed [5] studied Pakistani customers and found trust and credit card safety are major concerns.

6. Industrial Sector

Industry 5.0 focuses on smart manufacturing using IoT. Technologies like attack detection [53,54], smart control rooms [55–57], and digital twins [59] help improve security. Osak and Buzina [60] discussed how power systems must stay flexible and secure during digital upgrades, especially with more electric cars and renewable energy.

Mayhuasca and Sotelo [61] talked about how quantum technologies could make industries more secure and faster but are still expensive and complex. Raza et al. [62] looked at how companies balance preventing and responding to threats in digital projects, especially using Robotic Process Automation.

Trung et al. [63] discussed how IoT and AI are changing education, healthcare, tourism, and manufacturing. In schools, teachers use machine learning to track student progress. In health, big data speeds up public health services. However, these new tools bring security risks that need careful handling.

7. Diverse Organizational Contexts

Di et al. [64] suggested a new kind of network system using genetic algorithms to manage information security. Their method was better than traditional systems in terms of cost and speed. Alenezi [65] explained that software engineering is now a core part of building secure digital systems.

Marelli [66] said humanitarian groups using digital tools must be careful of cyber threats that can affect how they help people. Dvojmoč and Verboten [67] reminded companies of their duty to protect worker information using tools like firewalls and antivirus software. They also stressed the need to follow data protection laws like GDPR.

In environmental work, Mukhlynina et al. [68] studied how Russia is adding digital tech to environmental safety systems. They found problems like unclear laws, lack of funding, and poor infrastructure. Key success factors included skilled workers and good government policies.

Halabi et al. [69] recommended using green cybersecurity practices to reduce energy use. Voskresenskaya [70] studied how digital tools affect governance, economy, and society. They found digitalization helps with services, contracts, and online money, but poor data handling can slow progress. Governments should invest in infrastructure and make sure laws are in place to protect privacy.

Kuchumov et al. [71] said digital change can boost productivity but also bring risks like job loss or hacking. Regional policies should be tailored, not one-size-fits-all. Alahmadi et al. [72] talked about digital farming, which helps reduce manual work but has risks like side-channel attacks. Song et al. [73] added that IoT and 5G bring benefits to agriculture but can cause security problems. They proposed a secure way to gather data.

Gonçalves [74] noted that small businesses in accounting are starting to use digital tools, but cybersecurity remains a challenge. Tiron-Tudor et al. [75] said tools like AI and blockchain help with real-time audits, but companies must spend money to manage security risks.

Rodríguez-Abitia and Bribiesca-Correa [76] said technology is changing universities, and people may become content creators or influencers. Pavlova [77] said while education promotes open access to knowledge, it must now also focus on keeping digital systems secure.

Power systems are important in modern life but are also at risk of hacking [78,79]. Dagoumas [80] used IEEE models to study system stability under cyber threats. Diaba et al. [81] proposed a new model that outperformed traditional deep learning for detecting attacks in power grids. Presekal et al. [82] built a hybrid model using GC-LSTM and deep learning for finding problems in electric systems.

Kechagias et al. [83] showed how a maritime company found and fixed gaps in its cybersecurity by reviewing its strategy and handling risks systematically.

Sector	**Areas**	**Technologies Discussed**	**Challenges Identified**	**Key Studies/References**
Financial	Security in banking, online transactions, and money laundering detection	AI, Machine Learning, Blockchain, Cognitive Tech	Identity theft, low customer trust, fraud risks, limited blockchain analysis	[16]–[25]
Health	Patient privacy, secure medical devices, data handling in pandemics	Big Data, Blockchain, Cloud, AI, IoT, Biosensors	Data leaks, weak privacy controls, lack of staff training, increasing cyberattacks during COVID-19	[26]–[37]

Government	E-governance, digital services, national infrastructure protection	Digital ID, Tax Digitalization, Cognitive Systems	Uneven digital adoption, legal gaps, infrastructure issues, employee readiness	[38]–[45]
Business	E-commerce, cloud computing, employee involvement in tech, digital trust	IoT, AI, Blockchain, Cloud, Cybersecurity Frameworks (e.g., SWCSF)	Low digital skills, customer trust issues, high cost, cloud data breaches	[46]–[52]
Industrial	Smart manufacturing, energy systems, automation, digital resilience	IoT, Digital Twin, RPA, Quantum Tech, Machine Learning	Complex control systems, weak protocols, high cost of emerging tech, compliance challenges	[53]–[63]
Organizational	Enterprise security, secure development, software engineering, environmental safety	Genetic Algorithms, Secure DevOps, AI, Blockchain	Insecure data sharing, unclear regulations, lack of funding, digital divide across regions	[64]–[77]
Energy & Maritime	Cybersecurity in power grids, maritime infrastructure, and transport systems	Deep Learning (CNN, ANN, SVM), GC-LSTM, Fileless Attacks, APT techniques	Grid vulnerability, protocol-based attacks, advanced persistent threats (APT), cyber-defense planning	[78]–[83]

8. Cybersecurity framework for business organizations:

Based on our review, we propose a cybersecurity readiness framework for business organizations pursuing digital transformation

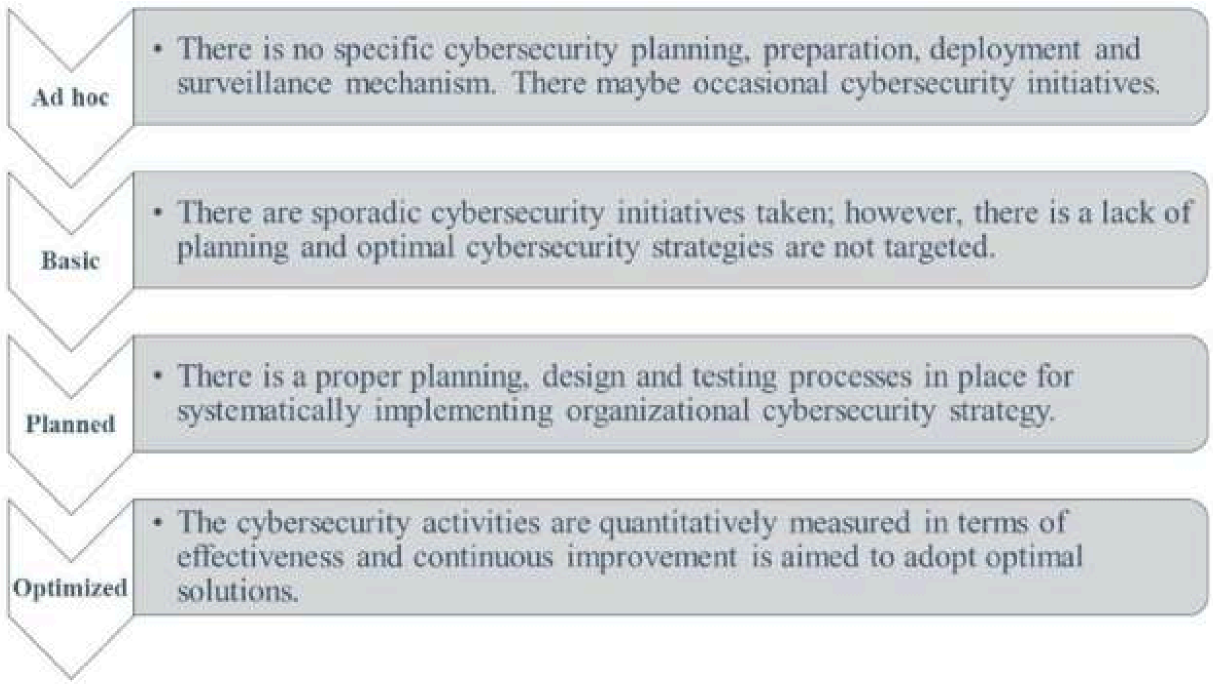


Figure 1. Cybersecurity readiness framework for business organizations.

At the ad hoc level, organizations do not have proper plans or systems in place to deal with cybersecurity threats. They lack preparation, deployment, and monitoring mechanisms. Cybersecurity in such organizations depends mostly on individual employee efforts, not formal strategies. As new technologies like artificial intelligence, big data, blockchain, and cloud services drive digital transformation, they also increase cybersecurity risks. But organizations at this level usually do not pay enough attention to these risks during their digital transformation journey.

At the basic level of the framework, organizations have some fundamental cybersecurity activities like basic planning, preparation, and monitoring. However, they do not have an official strategy or clear policy on cybersecurity. Their processes are not well-developed, and the efforts made are usually separate and uncoordinated. Also, there is no data or feedback available on how effective their cybersecurity methods are.

At the planned level, organizations have a proper cybersecurity strategy that defines how they will prepare for, deploy, and monitor their cybersecurity efforts. They regularly look for weaknesses by doing penetration testing or vulnerability scans. These organizations also recognize the importance of human factors in cybersecurity, so they provide ongoing training and awareness programs to employees. As new technologies like IoT devices, 5G, or quantum computing are introduced, they understand that new, unknown risks may appear. So, it becomes essential to carry out full risk assessments before applying these technologies.

At the optimized level, organizations constantly review and improve their cybersecurity systems for planning, preparation, implementation, and monitoring. Since technology and cyber threats evolve quickly, even strong security setups may develop gaps over time. Therefore, these organizations use forward-looking approaches, like forecasting future technologies and preparing cybersecurity plans ahead of time. This proactive mindset helps reduce future risks and supports safe and innovative digital transformation.

Conclusion:

References:

1. Hai, T.N., Van, Q.N., & Thi Tuyet, M.N. Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. Emerg. Sci. J., 2021, 5, 21– 36.
2. Möller, D. Cybersecurity in Digital Transformation: Scope and Applications. Springer: Berlin/Heidelberg, Germany, 2020.
3. Matt, C., Hess, T., & Benlian, A. Digital transformation strategies. Bus. Inf. Syst. Eng., 2015, 57, 339–343.
4. Saeed, S. Digital workplaces and information security behavior of business employees: An empirical study of Saudi Arabia. Sustainability, 2023, 15, 6019.
5. Saeed, S. A customer-centric view of e-commerce security and privacy. Appl. Sci., 2023, 13, 1020.
6. Sharif, M.H.U., & Mohammed, M.A. A literature review of financial losses statistics for cybersecurity and future trend. World J. Adv. Res. Rev., 2022, 15, 138–156.
7. Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. The economic cost of cybersecurity breaches: A broad-based analysis. In Workshop on the Economics of Information Security (WEIS), 2019, Boston, MA, USA, June 3–4.
8. Garg, V. Covenants without the sword: Market incentives for cybersecurity investment. In TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, 2021, Virtual, September 22–24.
9. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. Bus. Horiz., 2021, 64, 659–671.
10. Gordon, L.A., Loeb, M.P., & Zhou, L. Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model. J. Cybersecur., 2020, 6, tyaa005.
11. Krutilla, K., Alexeev, A., Jardine, E., & Good, D. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model. Risk Anal., 2021, 41, 1795–1808.

12. Simon, J., & Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. Eur. J. Oper. Res., 2020, 282, 161–171.
13. Uddin, M.H., Ali, M.H., & Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Manag., 2020, 22, 239–309.
14. Curti, F., Ivanov, I., Macchiavelli, M., & Zimmermann, T. City hall has been hacked! The financial costs of lax cybersecurity. SSRN. https://ssrn.com/abstract=4465071 (accessed June 15, 2023).
15. Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 2021, 372, n71.
16. Al-Alawi, A.I., & Al-Bassam, M.S.A. The significance of cybersecurity system in helping managing risk in banking and financial sector. J. Xidian Univ., 2020, 14, 1523–1536.
17. Hasan, M.F., & Al-Ramadan, N.S. Cyber-attacks and cyber security readiness: Iraqi private banks case. Soc. Sci. Humanit. J., 2021, 5, 2312–2323.
18. Joveda, N., Khan, M.T., Pathak, A., & Chattogram, B. Cyber laundering: A threat to banking industries in Bangladesh: In quest of effective legal framework and cyber security of financial information. Int. J. Econ. Financ., 2019, 11, 54–65.
19. Almudaires, F., & Almaiah, M. Data: An overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT), Amman, Jordan, July 14–15, pp. 732–738.
20. Smith, K.J., & Dhillon, G. Assessing blockchain potential for improving the cybersecurity of financial transactions. Manag. Financ., 2020, 46, 833–848.
21. Kuzmenko, O., Kubálek, J., Bozhenko, V., Kushneryov, O., & Vida, I. An approach to managing innovation to protect financial sector against cybercrime. Pol. J. Manag. Stud., 2021, 24, 276–291.
22. Rodrigues, A.R.D., Ferreira, F.A., Teixeira, F.J., & Zopounidis, C. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Res. Int. Bus. Financ., 2022, 60, 101616.
23. Fedorov, B.M., Fedorova, S.V., Zhang, H., & Mamedova, N.A. Using cognitive technologies to ensure the information security of banks in the conditions of digital transformation and development of biometrical identification. WSEAS Trans. Bus. Econ., 2023, 20, 382–387.
24. Patil, R., & Bharathi, S.V. A study on the business transformation, security issues and investors trust in fintech innovation. Cardiometry, 2022, 24, 918–932.
25. Rădulescu, C.V., Bodislav, D.A., & Negescu, M.D.O. The risks of digitization in the context of economic development and of ensuring social and informational security. In International Management Conference, 2019, Poznan, Poland, June 27–29, Volume 13, pp. 1040–1050.
26. Mijwil, M.; Aljanabi, M.; Ali, A.H. Chatgpt: Exploring the role of cybersecurity in the protection of medical information. Mesopotamian J. Cybersecur. 2023, 2023, 18–21.
27. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber attacks on healthcare devices using unmanned aerial vehicles. J. Med. Syst. 2020, 44, 29.

28. Buzdugan, A. Integration of cyber security in healthcare equipment. In Proceedings of the 4th International Conference on Nanotechnologies and Biomedical Engineering: Proceedings of ICNBME-2019, Chisinau, Moldova, 18–21 September 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 681–684.
29. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the Internet of medical things. Health Policy Technol. 2021, 10, 100549.
30. Abie, H. Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6.
31. Loi, M.; Christen, M.; Kleine, N.; Weber, K. Cybersecurity in health–disentangling value tensions. J. Inf. Commun. Ethics Soc. 2019, 17, 229–245.
32. Ali, K.A.; Alyounis, S. Cybersecurity in healthcare industry. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 695–701.
33. Abbas HS, M.; Qaisar, Z.H.; Ali, G.; Alturise, F.; Alkhalifah, T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. PLoS ONE 2022, 17, e0274550.
34. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. Technovation 2023, 121, 102583.
35. Paul, M.; Maglaras, L.; Ferrag, M.A.; AlMomani, I. Digitization of Healthcare Sector: A Study on Privacy and Security Concerns. ICT Express 2023, in press.
36. Nwaiwu, F.; Mbelu, S. Digital Transformation in Healthcare and Surveillance Capitalism: Comparative Assessment of Data and Privacy Protection Compliance across the European Union (5 July 2020). Available online: https://ssrn.com/abstract=3643838 (accessed on 15 June 2023).
37. Maleh, Y.; Mellal, B. Digital transformation and cybersecurity in the context of COVID-19 proliferation. IEEE Technol. Policy Ethics 2021, 6, 1–4.
38. Shaheen, K.; Zolait, A.H. The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. Inf. Comput. Secur. 2023. ahead-of-print.
39. Montasari, R. Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity; Springer Nature: Berlin/Heidelberg, Germany, 2023; pp. 7–25.
40. Alhalafi, N.; Veeraraghavan, P. Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. Smart Cities 2023, 6, 1523–1544.
41. Al Shobaki, M.J.; El Talla, S.A.; Al Najjar, M.T. Digital Transformation and Its Impact on the Application of Cyber Security in the Ministry of Interior and National Security in Palestine. 2022. Available online: http://www.moi.gov.ps (accessed on 15 June

2023).
42. Al Najjar, M.T.; Al Shobaki, M.J.; El Talla, S.A. The Reality of Digital Transformation in the Palestinian Ministry of Interior and National Security. 2022. Available online: www.ijeais.org/ijamsr (accessed on 15 June 2023).
43. Fjord, L.B.; Schmidt, P.K. The Digital Transformation of Tax Systems: Progress, Pitfalls and Protection in a Danish Context. 2022. Available online: https://ssrn.com/abstract=4252832 (accessed on 15 June 2023).
44. Mijwil, M.; Filali, Y.; Aljanabi, M.; Bounabi, M.; Al-Shahwani, H. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. Mesopotamian J. Cybersecur. 2023, 2023, 1–6.
45. Maglaras, L.; Kantzavelou, I.; Ferrag, M.A. Digital Transformation and Cybersecurity of Critical Infrastructures. Appl. Sci. 2021, 11, 8357.
46. Bokhari, S.; Hamrioui, S.; Aider, M. Cybersecurity strategy under uncertainties for an IoE environment. J. Netw. Comput. Appl. 2022, 205, 103426.
47. Gonchar, V. The Transformation of Entrepreneurial Activity in the Conditions of the Development of the Digital Economy and a Methodology of Assessing Its Digital Security in Digital Technologies in the Contemporary Economy: Collective Monograph; Simanavičienė, Ž., Ed.; Mykolas Romeris University Research: Vilnius, Lithuania, 2022; ISBN 9786094880506. [Google Scholar]
48. Kuzior, A.; Vasylieva, T.; Kuzmenko, O.; Koibichuk, V.; Brożek, P. Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. J. Open Innov. Technol. Mark. Complex. 2022, 8, 195.
49. Putri MS, D.; Gultom, R.A.; Wadjdi, A.F. The Concept of an Electronic-Based Government System and the Six-Ware Cyber Security Framework in Supporting the Digitization of the Indonesian Government. Def. Secur. Stud. 2023, 4, 1–7.
50. Shitta-Bey, A.M. Security Concerns of Cloud Migration and Its Implications on Cloud-Enabled Business Transformation Effect of Quality Education on Poverty Alleviation View Project.
Master's Thesis, Università della Svizzera Italiana, Lugano, Switzerland, 2023. Available online: https://www.researchgate.net/publication/369118961 (accessed on 15 June 2023).
51. Trung, N.D.; Huy DT, N.; Van Thanh, T.; Thanh NT, P.; Dung, N.T.; Thanh Huong, L.T. Digital transformation, AI applications and IoTs in Blockchain managing commerce secrets: And cybersecurity risk solutions in the era of industry 4.0 and further. Webology 2021, 18, 10–14704.
52. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi
Arabia. Electronics 2022, 11, 293.
53. Anthi, E.; Williams, L.; Rhode, M.; Burnap, P.; Wedgbury, A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J. Inf. Secur. Appl. 2021, 58, 102717.

54. Meeran, Y.A.; Shyry, S.P. Resilient Detection of Cyber Attacks in Industrial Devices. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; pp. 564–569.
55. Ameri, K.; Hempel, M.; Sharif, H.; Lopez Jr, J.; Perumalla, K. Design of a novel information system for semi-automated management of cybersecurity in industrial control systems. ACM Trans. Manag. Inf. Syst. 2023, 14, 1–35.
56. Buja, A.; Apostolova, M.; Luma, A. Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment. In Proceedings of the 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 14 June 2023; pp. 1–5. [Google Scholar]
57. Ramirez, R.; Chang, C.K.; Liang, S.H. PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. Electronics 2023, 12, 1195.
58. Zanasi, C.; Russo, S.; Colajanni, M. Flexible Zero Trust Architecture for the Cybersecurity of Industrial Iot Infrastructures. Available online: https://ssrn.com/abstract=4481853 (accessed on 15 June 2023).
59. Jacopo, P.; Graziana, C.; Federica, P.; Giarrè, L. Using Digital Twin to Detect Cyber-Attacks in Industrial Control Systems. In Proceedings of the IEEE Proceedings of 2023 EUROCON, Torino, Italy, 6–8 July 2023.
60. Osak, A., & Buzina, E. Flexibility and security of power systems, methods of analysis, and criteria for their evaluation in the conditions of digital transformation of the power industry. AIP Conference Proceedings, 2023, 2552, 040008.
61. Mayhuasca, J., & Sotelo, S. Quantum technologies for digital transformation and informatica security. International Journal of Engineering Science, 2022, 15, 43–50.
62. Raza, H., Baptista, J., & Constantinides, P. Conceptualizing the role of IS security compliance in projects of digital transformation: Tensions and shifts between prevention and response modes. In ICIS, 2019, Houston, TX, USA.
63. Trung, N.D., Huy, D.T.N., & Le, T.H. IoTs, machine learning (ML), AI and digital transformation affects various industries—principles and cybersecurity risks solutions. Management, 2021, 18, 10–14704.
64. Di, Z., Liu, Y., & Li, S. Networked organizational structure of enterprise information security management based on digital transformation and genetic algorithm. Frontiers in Public Health, 2022, 10, 921632.
65. Alenezi, M. Software and security engineering in digital transformation. arXiv preprint, 2021, arXiv:2201.01359.
66. Marelli, M. Hacking humanitarians: Defining the cyber perimeter and developing a cybersecurity strategy for international humanitarian organizations in digital transformation. International Review of the Red Cross, 2020, 102, 367–387.
67. Dvojmoč, M., & Verboten, M.T. Cyber (in) security of personal data and information in times of digitization. Medicine, Law & Society, 2022, 15, 287–304.
68. Zarapina, L., Mukhlynina, M., Adamenko, A., Mukhlynin, D., & Belokopytova, N. Issues of legal support of socio-economic policy and environmental security of Russia in the context of digital transformation. In Proceedings of the International Scientific-Practical Conference, 2021, Kirov, Russia, June 17–18, pp. 336–340.

69. Halabi, T., Bellaiche, M., & Fung, B.C. Towards adaptive cybersecurity for green IoT. In Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), 2022, Bali, Indonesia, November 24–26, pp. 64–69.

70. Voskresenskaya, E., Vorona-Slivinskaya, L., & Panov, S. Digital transformation of social sector as the factor of development and security of the country. E3S Web of Conferences, 2019, 135, 03075.

71. Kuchumov, A., Pecherictsa, E., Chaikovskaya, A., & Zhilyaeva, I. Digital transformation in the concept of economic security of Russia and its regions. In Proceedings of the 2nd International Scientific Conference on Innovations in Digital Economy, 2020, St. Petersburg, Russia, October 22–23, pp. 1–8.

72. Alahmadi, A.N., Rehman, S.U., Alhazmi, H.S., Glynn, D.G., Shoaib, H., & Solé, P. Cyber-security threats and side-channel attacks for digital agriculture. Sensors, 2022, 22, 3520.

73. Song, J., Zhong, Q., Wang, W., Su, C., Tan, Z., & Liu, Y. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sensors Journal, 2020, 21, 17430–17438.

74. Gonçalves, M.J.A., da Silva, A.C.F., & Ferreira, C.G. The future of accounting: How will digital transformation impact the sector? Informatics, 2022, 9, 19.

75. Tiron-Tudor, A., Donțu, A.N., & Bresfelean, V.P. Emerging technologies' contribution to the digital transformation in accountancy firms. Electronics, 2022, 11, 3818.

76. Rodríguez-Abitia, G.; Bribiesca-Correa, G. Assessing digital transformation in universities. Future Internet 2021, 13, 52.

77. Pavlova, E. Enhancing the organisational culture related to cyber security during the university digital transformation. Inf. Secur. 2020, 46, 239–249.

78. Ribas Monteiro, L.F.; Rodrigues, Y.R.; Zambroni de Souza, A.C. Cybersecurity in Cyber–Physical Power Systems. Energies 2023, 16, 4556.

79. Liang, J.; Zhu, H.; Zhang, B.; Liu, L.; Liu, X.; Lin, H.; Tian, J.; Chen, Q. Research and Prospect of Cyber-Attacks Prediction Technology for New Power Systems. In Proceedings of the 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 24–26 February 2023; Volume 6, pp. 638–647.

80. Dagoumas, A. Assessing the impact of cybersecurity attacks on power systems. Energies 2019, 12, 725.

81. Diaba, S.Y.; Shafie-Khah, M.; Elmusrati, M. Cyber Security in Power Systems Using MetaHeuristic and Deep Learning Algorithms. IEEE Access 2023, 11, 18660–18672.

82. Presekal, A.; Ştefanov, A.; Rajkumar, V.S.; Palensky, P. Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Trans. Smart Grid 2023. Early Access.

83. Kechagias, E.P.; Chatzistelios, G.; Papadopoulos, G.A.; Apostolou, P. Digital transformation of the maritime industry: A cybersecurity systemic approach. Int. J. Crit. Infrastruct. Prot. 2022, 37, 100526.

Iqra(Author)
MY University Islamabad Pakistan

Hafiz Muhammad Naveed(Co-Author)

Reshaping Human Resource Management in the Age of AI and Global Disruption: Challenges, Ethics, and the Future of World.

Abstract:

Two opposing forces the quick integration of artificial intelligence (AI) and the beginning of global upheavals, including pandemics, climate disasters, economic instability, and political unrest are radically altering human resource management (HRM). This article offers a thorough, multidisciplinary examination of how artificial intelligence is changing conventional HR tasks, from talent acquisition and performance management to learning and employee engagement, as worldwide disturbances compel a parallel reimagining of HRM as a strategic, ethical, and future-oriented discipline. Using critical thinking and worldwide case studies, we examine developing problems connected to algorithmic bias, data privacy, emotional labor, neurodiversity, hybrid labor, and legislative complexity. The article suggests systems for ethical integration of artificial intelligence in HR, digital literacy development, culturally astute leadership, and resilient workplace ecosystems. Last but not least, it provides forward-looking suggestions for HR experts, business leaders, and lawmakers to help to design an equitable, sustainable, and people-centric future of employment.

Keywords: Artificial Intelligence in HR, Human Resource Transformation, Global Workforce Disruption, Hybrid Work Models, Ethical HR Practices, Future of Work, Neurodiversity and Inclusion and Sustainable Human Resource Management.

1 PhD research scholar And visiting lecturer my

university Islamabad(+923144482484)naveed.khilji786@gmail.com

2 Master in International Relation (IR).

Independent scholar (+923153957080) email: Naveed.khilji786@gmail.com.

Ugochukwu Ezenwa Urenyere(Author) *Kabani Holdings LTD*	**Big Data and AI as Catalysts for Africa's Digital Transformation**

Abstract

Digital transformation in Africa is gaining pace, although there has been a consistent problem in closing the digital divide, as well as utilizing emerging technologies such as Big Data and Artificial Intelligence (AI) to generate growth that is inclusive of Africa. This research focuses on the current state of AI and Big Data implementation in the most critical spheres on the African continent: agriculture, healthcare, finance, and urban development, highlighting both opportunities and systemic challenges. The research uses literature review, case study (e.g., M-Pesa, Zipline), and policy analysis because they are mixed methods. It determines critical success factors and implementation challenges. The results demonstrate that although innovative AI-based solutions are transforming industries such as mobile banking, precision farming, the existing infrastructure gaps, lack of skills, and regulatory failure are the barriers to their large-scale adoption.

As the study shows, one of the ways that could speed up the deployment of technology in an equitable manner is the use of public-private partnerships and specific policy measures. The major lessons are that a localized AI training program is required, the growth of digital infrastructure, and the development of strong data governance frameworks. In this paper, I have addressed the issue of the Fourth Industrial Revolution in Africa and presented practical recommendations to policymakers, investors, and entrepreneurs who will discuss/visit GCABT 2025, focusing on how Africa should respond to achieve its sustainable development.

Introduction

Africa is at a pivotal point between the digitalisation of the continent, and this is where the use of Big Data and Artificial Intelligence (AI) can mend structural infrastructural gaps and open the sustainable development. As reported by Echendu & Okafor (2021), the uneven availability of the internet, power outage, and lack of technical means are some of the challenges stemming from the rapid urbanization and mobile penetration on the continent that affect the effective utilization of these technologies. The paper is an innovative analysis of the application of AI and Big Data in the most important spheres, such as agriculture, healthcare, finance, and smart cities, with the success stories of M-Pesa fintech innovations and Zipline based on AI-enabled medical deliveries. Using the assessment of the existing implementations, the study proposes specific measures to facilitate inclusive growth in terms of policy implications that should make the process of inclusive growth quicker.

Related Studies

Bestowed with great scholarly interest, Artificial Intelligence (AI) and Big Data leverage in developing economies have been on the hot seat and especially in terms of how they can spur inclusive growth. According to Arakpogun et al. (2021), studies show that AI can boost productivity in cases where the resources are scarce, but they state that scaling due to a lack of infrastructure is generally an issue. In Africa, it can be seen that mobile-first economies as Kenya and Nigeria, have been able to bypass all the conventional development paths due to the utilization of Big Data analytics in the fields of finance and agriculture (Anning-Dorson, 2025). Pasipamire & Muroyiwa (2024) warn, however, that unless specific AI training data is available, the algorithms will not consider the specific situation of the African continent, and they will contribute to worsening biases in the prediction systems (like healthcare or credit scoring), never mind the rest of the socio-economic situations.

Big Data has been revolutionary in African fintech, especially in the area of offering alternative credit scoring to the unbanked. Mulili (2022) records the use of the transactional information of platforms such as M-Pesa to render microloan opportunities, which has lessened the financial inclusion by 27% in East Africa. Likewise, Agritech applications, discussed by Mihret et al. (2025), show that the use of satellite-based imagery and Internet of Things in the form of sensors helps smallholder farmers to maximize irrigation efficiency, increasing yields by 20-35% in such countries as Ghana and Rwanda. However, in all these developments, Giller et al. (2021) brings out one major missing point that is, most agricultural technology solutions are only directed to commercial farmers, leaving out subsistence farming, which forms 60% of the African rural economy.

One research gap that has persisted is a rural-urban gap in the availability of technology. Although the rate of urban adoption of AI in Africa is equal to that of the rest of the world (Mwansa et al., 2025), there is a gap in rural locations caused by the lack of electricity (only 43% is covered) and low broadband penetration (28%). Adegoke et al. (2025) note that the current research has been concentrated disproportionately on tech hubs (e.g., Lagos, Nairobi) and, as a result, 12 less developed countries lack representation in AI policy discussion. Moreover, Calzati (2022) is afraid of data colonialism, when foreign companies benefit at the expense of African data without developing local capacity. This aspect is also mentioned by the African Digital Rights Network when criticizing AI baseline surveillance measures.

In the attempt to fill these gaps, researchers such as Mwansa et al. (2025) propose the idea of homegrown AI ecosystems, which implies the assistance of the government through public-private partnerships. The development in the future should give primary importance to the contextualized solutions of contextualized solutions, like Swahili-language NLP or off-grid AI tools, to guarantee equitable gains. This paper advances these approaches through the intellectually sustained analysis of locally tailored AI/Big Data applications that are scalable and a range of policy frameworks capable of narrowing the gap between urban and rural.

Methodology

The proposed study will use a qualitative approach of secondary data analysis, which is a research methodology, to determine the adoption and the effects of the application of Big Data and AI technologies in Africa (Cheong et al., 2023). The three major sources of primary data include (1) the industry reports by the reputable organizations (e.g., the GSMA, World Bank, and African Development Bank (AfDB)), which entail macroeconomic and sector-specific analysis of trend patterns in digital adoption; (2) the peer-reviewed journal papers on AI governance and ethical issues in developing economies; and (3) successful implementation case studies that can serve as examples (e.g., the AI-based financial inclusion strategy of M-Pesa in Kenya or the drone-based medical supply chain of Zipline in R The sources have been chosen because of their reliability, relevance, and topicality (last five years of publication).

In order to evaluate the opportunities and challenges of AI and Big Data implementation in a methodical assessment, the present study uses a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis framework. According to this approach, it is possible to systematically analyze both internal factors (e.g., mobile-first economy of Africa as the strength, the shortage of skills as a weakness) and external factors (e.g., the trend of worldwide investing as the opportunity, the risk of data privacy as the threat). SWOT analysis is complemented with comparative case study analysis to determine the best practices and the barriers to scalability.

The data triangulation was done by cross-checking reports of findings from various sources to ensure that the results were methodologically rigorous. Also, practical constraints, including the possible bias of industry-funded reports and the absence of unified measures of AI adoption, are mentioned. Such an approach will underpin the evidence-based basis of drawing policy recommendations and strategic implications on behalf of GCABT 2025 stakeholders.

Result

The empirical evidence included in this section shows both the transforming significance of Big Data and AI throughout Africa, and ongoing discrepancy in the implementation and infrastructure across the continent. The visual information which is of great source of analysis offers a very irresistible story that fits the theme of this paper, which is; innovation, inequality and the potentialities of the respective sector.

Top 10 Funded Startups - Africa - 2017

Startups	Country	Industry	Amount ($M)
PEG	Ghana	Solar/Fintech	13.5
Twiga	Kenya	B2B Commerce/ Supply Chain	10.3
Flutterwave	Nigeria	Fintech	10
iot.nxt	South Africa	IOT	7.7
solar now	Uganda	Solar Energy	6
Vezeeta	Egypt	HealthTech	5
CARS45	Nigeria	eCommerce	5
we think code_	South Africa	Social Impact/ EdTech	4.5
BitPesa	Kenya	Fintech	4.5
OOLU	Senegal	Solar Energy	3.2
* Andela	Nigeria/USA	EdTech	40

*The Startup is based in Nigeria and incorporated in the USA
** This infographic is a part of Weetracker's African Startup Funding Report 2017

Figure 1: Top Funded Startups of Africa – 2017 Source: (https://weetracker.com/2018/01/08/top-funded-startups-of-africa-2017/)

As shown above (Figure 1), the very formative concentration of venture capital in a very few major markets of Nigeria, Kenya, and South Africa accounted for more than 80% of the Startup funding at the time. Although this is outdated, the image helps us understand the origin of the current AI ecosystem by explaining how past investment trends have created modern-day tech centers.

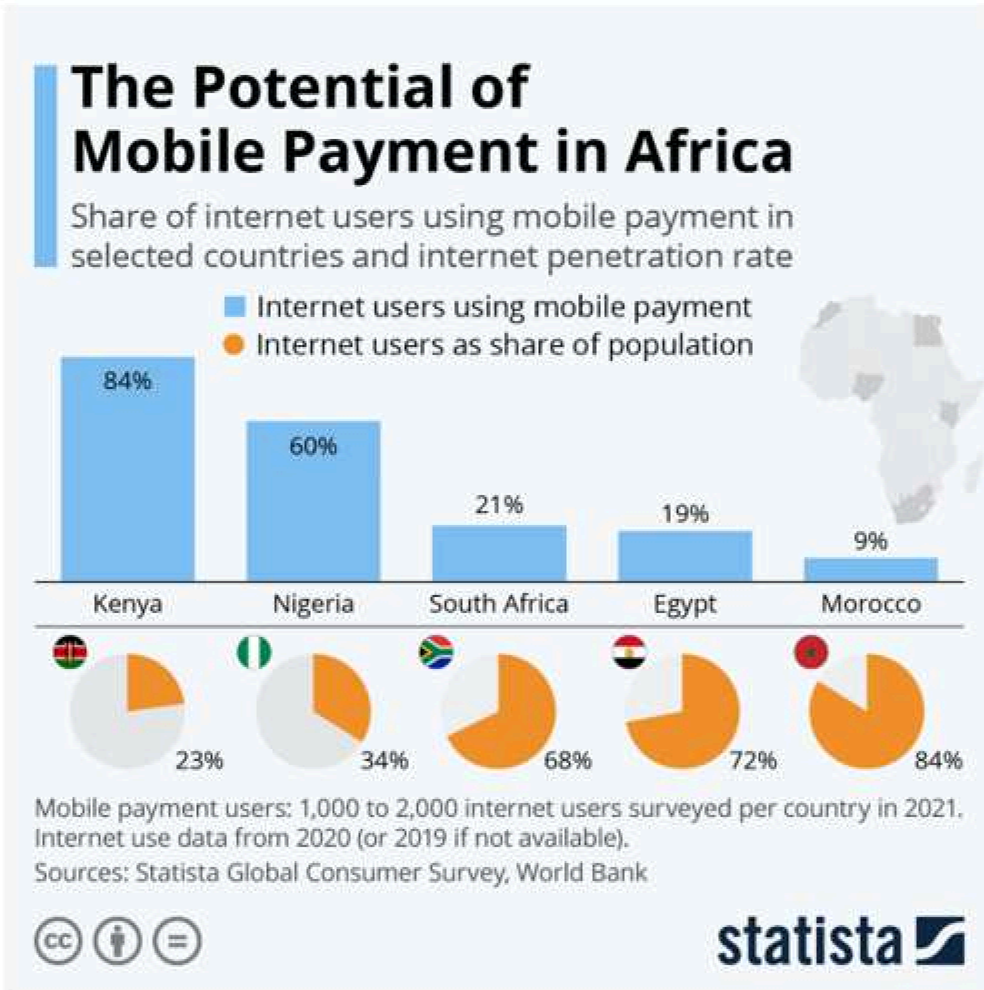


Figure 2: The Potential of Mobile Payment in Africa Source: (https://www.statista.com/chart/27017/mobile-payment-in-africa/)

The majority of firms in fintech and e-commerce as sources of data reflect further in later years this sectoral specialisation because, in the figure above (The Potential of Mobile Payment in Africa), one observes the leadership role of M-Pesa in mobile money. The increase in the trend of mobile payment adoption (12% in 2010, and 48% in 2022) represented by this graph outright confirms the argument presented in the paper regarding the possibility of leapfrogging conventional banking systems with AI-based solutions.

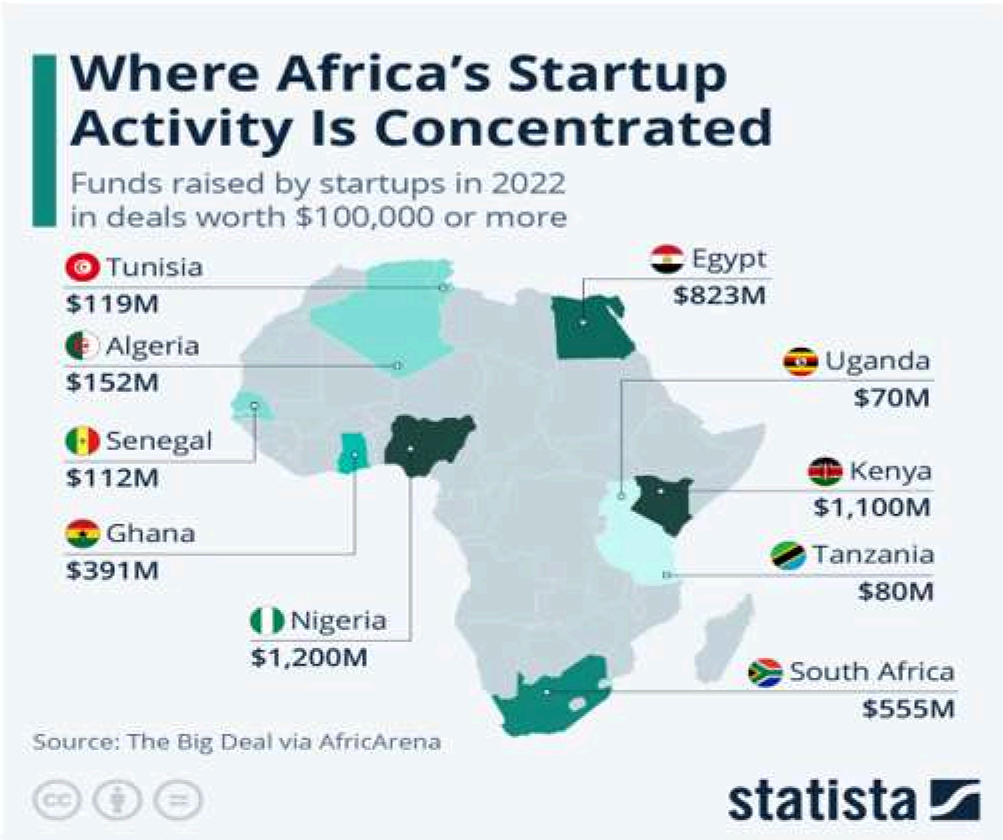


Figure 3: Where Africa's Startup Activity Is Concentrated Source: (https://www.statista.com/chart/24911/vc-investment-by-country-in-africa/)

Figure 3 (Where Africa Startup Activity Is Concentrated) brings this story up to date with current geographical distribution figures, with Nigeria (42% of investments) again taking a commanding position, but Rwanda, Côte d'Ivoire, Egypt, and Morocco all increasing their activity. The visual is a pronounced depiction of urban technology centers falling to the disservice of areas, which consolidates the infrastructural issues.

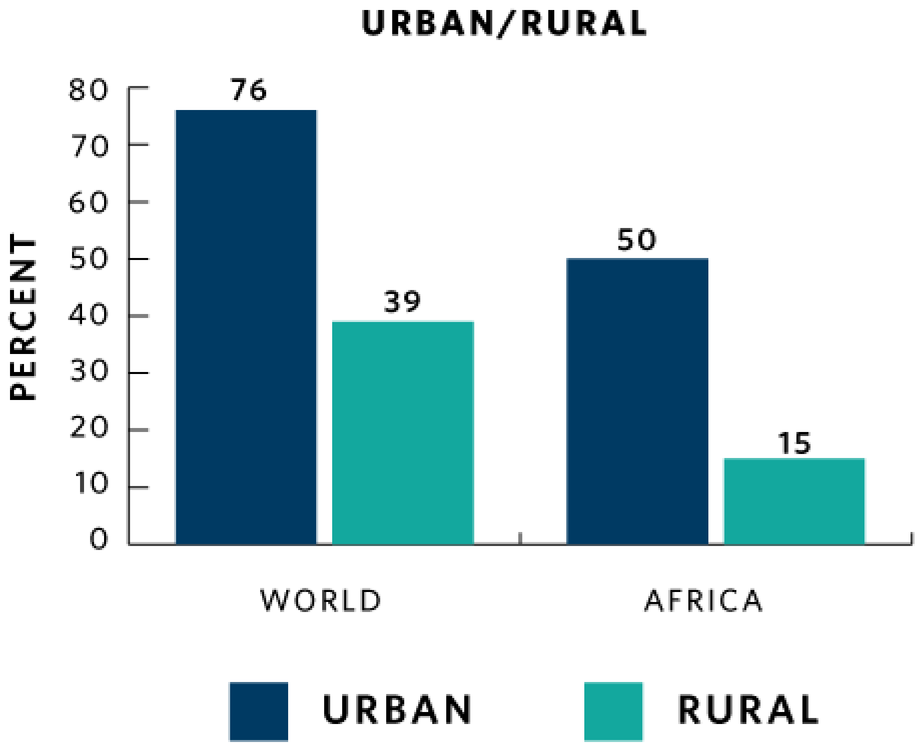


Figure 4: Internet usage differences in Africa by demographics, 2022. Source: (https://www.researchgate.net/figure/Charts-showing-the-Internet-usage-differences-in-Africa-by-demographics-Source-Munga_fig2_373433110)

The imbalance is further measured in Figure 4 (Internet Usage Differences in Africa by Demographics, 2022), whereby rural penetration of the internet is 28% against 63% in urban areas. The division of the graph by age and gender also reveals the risks of exclusion since women and older segments of the population are overrepresented, which is an essential aspect of fair AI implementation.

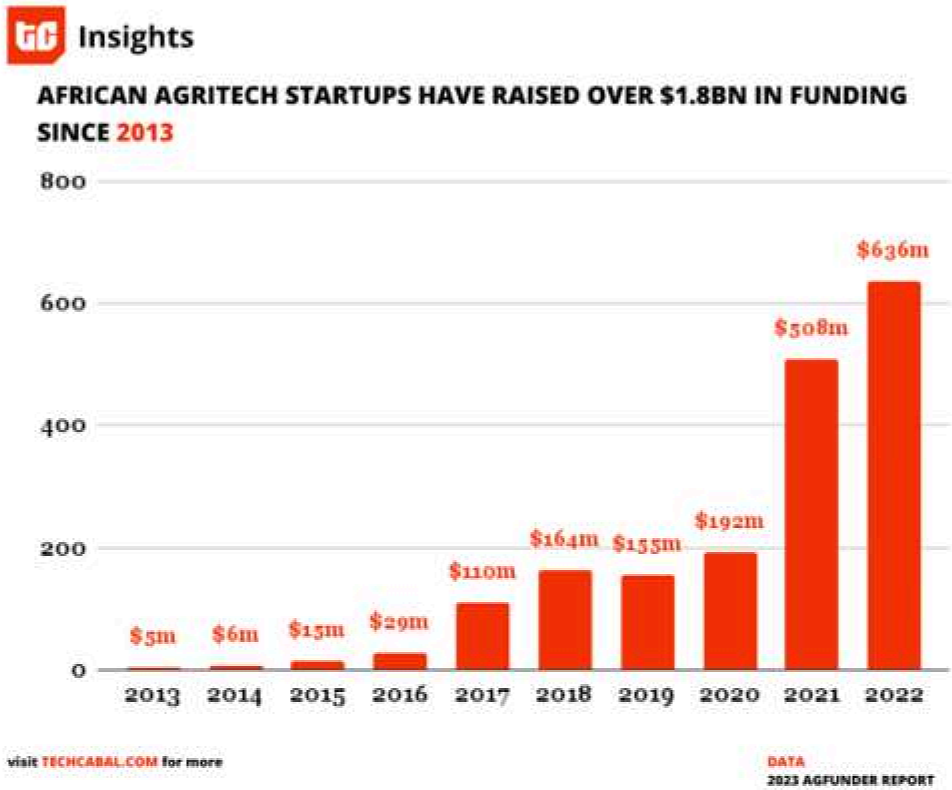


Figure 4: Exploring AI-driven solutions for African agriculture. Source: (https://insights.techcabal.com/exploring-ai-driven-solutions-for-african-agriculture/)

The breakthroughs identified on a sector basis are presented in Figure 5 (Exploring AI-Driven Solutions in African Agriculture) and include solutions by building intelligent farming systems, such as soil sensors and predictive analytics. The idea that the image focuses on the role of smallholder farmers resonates with the case study in the paper that portrays Twiga Foods and their work with the use of AI to optimize their supply chains and minimize post-harvest waste. Likewise, the data on mobile payments provided in Figure 5 is used to supplement the discussion of the AI-supported credit scoring that M-Pesa is likely to make available to 20 million more users (Bischoff et al., 2024). Collectively, these images prove the thesis of the paper that AI in specific fields will be able to solve the systematic gaps in agriculture and finance.

Nevertheless, the pictures portray inconsistencies as well. Although Figures 1-2 depict colorful Startup ecosystems, the connectivity voids in Figure 3 identify the obstacles to the scalability of these innovations. This is a tension that also supports the policy recommendations of this paper: unless investments in rural broadband and electricity are made, the benefits of AI will be confined to cities. The imagery unanimously contributes to the case that advocates twofold action: the one promoting local markers of success, and the one that is looking beyond structural disparities.

In short, such numbers make abstract arguments real. The stages of the African AI story are how they depict the progress of powered startups (Figure 1) to seasoned industry applications (Figures 4 and 5) with Figure 3 a cruel reminder of incomplete work on infrastructure. To the GCABT participants, this visual story is a coalescence of the urgency and opportunity to change Africa to a digital continent.

Discussion

The findings demonstrate the notable variance in AI and Big Data usability in the African sectors, with agricultural and fintech industries taking the lead on the one hand, and education being at the bottom of the list on the other hand. According to Figure 5, which illustrates the growth of mobile payment in fintech, the success of Fintech lies in its effectiveness in addressing the mobile-first economy of Africa and the direct benefit it delivers to the unbanked community (Bischoff et al., 2024). On the same note, agricultural technologies prosper because of their concrete influence in terms of food security and income generation through the AI-driven farming instruments, as is illustrated in Figure 4. Conversely, education is being adopted at a slower rate because of infrastructural obstacles (e.g., low access to the internet among schools in rural areas, as depicted in Figure 3) and difficulty in merging AI with the formal curricula.

There are also ethical issues with this disproportionate development. The fact that the startups are concentrated in city centers (Figures 1-2) poses a risk of further inequality because the rural population, which is disadvantaged by gaps in connectivity (Figure 3), does not see the benefits of AI. Data security is still very tentative since, out of 54 African nations, only 12 are strongly established in the protection act Kariuki et al. (2023), exposing users to the risk of being exploited. Along with the overall success of this sector, despite all the stated progress, there is still a possibility that algorithmic bias leads to discrimination against women and low-income groups depicted in fintech credit scoring.

The policymakers need to mitigate such inequalities by investing specifically in education infrastructure and strong data governance systems that would create even growth. As shown in Figure 5, the success of mobile money shows that when solutions meet local needs and possibilities, adoption is going to occur. With the implementation of these lessons in the case of late sectors, coupled with ethical risks reduction, Africa can use AI and Big Data as actual instruments of inclusive growth.

Conclusion

This paper proves that Big Data and Artificial Intelligence are causing revolutionary change in Africa, especially in the agricultural sector, healthcare, and financial services, but the use of technology is not evenly distributed because of a lack of availability of infrastructure and talent supply. To keep up this pace, we suggest ourselves localized AI training courses to establish in-country talent and one-time infrastructure financing where the rural and urban can be connected. We invite GCABT 2025 participants, who are policymakers, investors, and innovators, to work on scalable solutions that guarantee inclusive growth and make Africa a world leader in the ethical and sustainable development of AI.

References

Adegoke, D., Ismail, O., Joshua, T., & Solaja, O. (2025). Exploring Digital, Artificial Intelligence and Emerging Technology Inequality in Nigeria and Sub-Saharan Africa: A Review of Key Issues and Challenges. *The Palgrave Handbook of Global Social Problems*, 1-21. https://doi.org/10.1007/978-3-030-68127-2_606-1

Anning-Dorson, T. (2025). The Evolution and Impact of Business Models in Africa's Emerging Digital Economy. In *Digital Business Transformation in Africa, Volume I: Business Model Innovation* (pp. 35-74). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-91756-1_3

Arakpogun, E. O., Elsahn, Z., Olan, F., & Elsahn, F. (2021). Artificial intelligence in Africa: Challenges and opportunities. *The fourth industrial revolution: Implementation of artificial intelligence for growing business success*, 375-388. https://doi.org/10.1007/978-3-030-62796-6_22

Bischoff, C., Kamoche, K., & Wood, G. (2024). The Formal and Informal Regulation of Labor in AI: The Experience of Eastern and Southern Africa. *ILR Review*, *77*(5), 825-835. https://doi.org/10.1177/00197939241278956c

Calzati, S. (2022). ‘Data sovereignty’or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs: a document review on Kenya. *Journal of Contemporary African Studies*, *40*(2), 270-285. https://doi.org/10.1080/02589001.2022.2027351

Cheong, H. I., Lyons, A., Houghton, R., & Majumdar, A. (2023). Secondary qualitative research methodology using online data within the context of social sciences. *International Journal of Qualitative Methods*, *22*, 16094069231180160. https://doi.org/10.1177/16094069231180160

Echendu, A. J., & Okafor, P. C. C. (2021). Smart city technology: a potential solution to Africa's growing population and rapid urbanization?. *Development Studies Research*, *8*(1), 82-93. https://doi.org/10.1080/21665095.2021.1894963

Giller, K. E., Delaune, T., Silva, J. V., Descheemaeker, K., Van De Ven, G., Schut, A. G., ... & van Ittersum, M. K. (2021). The future of farming: Who will produce our food?. *Food Security*, *13*(5), 1073-1099. https://doi.org/10.1007/s12571-021-01184-6

Kariuki, P., Ofusori, L. O., & Subramaniam, P. R. (2023). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. *Security Journal*, 1. https://doi.org/10.1057/s41284-023-00378-1

Mihret, Y. C., Takele, M. M., & Mintesinot, S. M. (2025). Advancements in agriculture 4.0 and the needs for introduction and adoption in Ethiopia: a review. *Advances in Agriculture*, *2025*(1), 8828400. https://doi.org/10.1155/aia/8828400

Mulili, B. M. (2022). Digital financial inclusion: M-PESA in Kenya. In *Digital business in Africa: Social media and related technologies* (pp. 171-191). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93499-6_8

Mwansa, G., Ngandu, M. R., & Mkwambi, Z. (2025). Bridging the digital divide: exploring the challenges and solutions for digital exclusion in rural South Africa. *Discover Global Society*, *3*(1), 54. https://doi.org/10.1007/s44282-025-00189-2

Pasipamire, N., & Muroyiwa, A. (2024). Navigating algorithm bias in AI: ensuring fairness and trust in Africa. *Frontiers in Research Metrics and Analytics*, *9*, 1486600. https://doi.org/10.3389/frma.2024.1486600

Shilin Chhabra(Author) *University of Wisconsin-Madison*	**Secure, Scalable and Reproducible Cloud-Native AI Workflows for Data-Intensive Science**

Abstract

Scientific discovery increasingly depends on AI-driven workflows that must process massive datasets and deploy complex models across heterogeneous environments. Traditional HPC pipelines often struggle with elastic scaling, rigorous reproducibility, and end-to-end security. This paper presents a cloud-native blueprint that integrates containerization, Kubernetes orchestration, and GitOps-based CI/CD to modularize data ingestion, preprocessing, training, inference, and visualization into version-controlled microservices reinforced by zero-trust controls and continuous vulnerability scanning. We validate the design via an AI-driven $PM_{2.5}$ air-quality forecasting workflow using OpenAQ and NOAA data. The system achieves nearlinear scale-out, low-latency inference (~150 ms), and end-to-end reproducibility through image digests and checksummed datasets. Results indicate that cloud-native infrastructures can deliver enterprise-grade security and scientific traceability while accelerating AI-enabled discovery. We conclude with guidance for cost/energy modeling, hybrid HPC–cloud interoperability, FAIR data governance, and trustworthy AI gates within CI/CD.

Keywords: cloud-native, scientific workflows, Kubernetes, GitOps, MLOps, reproducibility, zero-trust security, air quality

1. Introduction

Scientific workflows - DAGs of tasks with explicit data/control dependencies - structure complex analyses across domains from astronomy to bioinformatics (Ivie & Thain, 2018). In parallel, cloud-native architecture leverages microservices, containers, and declarative APIs to obtain elasticity and manageability, while AI-driven modeling embeds machine learning to deliver predictive insight at scale.

Modern research is data- and compute-intensive. Upcoming experiments (e.g., HL-LHC) will generate exascale data, outstripping static, batch-scheduled HPC pipelines (ATLAS Collaboration, 2020; Gutsche et al., 2023). Cloud platforms offer elastic compute/storage that aligns with bursty AI workloads and shortens queue delays.

However, migration is non-trivial. First, scalability: monolithic HPC stacks with fixed allocations resist horizontal scale common in AI services. Second, reproducibility: "workson-my-machine" failure modes persist without portable environments and provenance (Ivie & Thain, 2018; Kanwal et al., 2017). Third, security: multi-user research systems often prioritize performance over least-privilege design and supply-chain controls (NIST, 2020, 2023). Containers and orchestration can help if combined with systematic versioning, policy enforcement, and runtime monitoring.

Contributions. We propose a unified, cloud-native architecture that (i) decomposes workflows into containerized microservices managed by Kubernetes; (ii) operationalizes GitOps + CI/CD for end-to-end reproducibility; and (iii) embeds zero-trust controls (RBAC, NetworkPolicies, image scanning, runtime detection). A $PM_{2.5}$ case study demonstrates feasibility and performance.

2. Background and Related Work

Reproducibility. Reproducibility remains uneven in computational science due to hidden dependencies, changing libraries, and weak provenance capture (Ivie & Thain, 2018; Kanwal et al., 2017). Workflow systems (Galaxy, Snakemake, Nextflow, Airflow) formalize pipelines, but environment assumptions often remain implicit, hampering portability.

Scalable AI stacks. Distributed engines - Spark MLlib, Ray, and Dask - compose parallel pipelines and scale training and hyperparameter tuning across clusters. Kubernetes has become the substrate for elastic ML services, with Kubeflow exposing K8s-native constructs for pipelines and distributed training (Spark, Ray, GPU/TPU nodes).

Workflow & MLOps frameworks. Kubeflow Pipelines, MLflow, Argo Workflows, Pachyderm, and Airflow cover pipeline definition, experiment tracking, data versioning, and scheduling. Yet most solutions address slices of the lifecycle; few offer an integrated blueprint that couples reproducibility and security by design.

Container security. Studies report frequent vulnerabilities in scientific images and stress supply-chain hardening, minimal base images, and continuous scanning (Kaur et al., 2020; Javed et al., 2021). Operational zero-trust further requires strong identity, mTLS, policy-ascode, and runtime detection (NIST, 2020, 2023).

Gap. Prior work demonstrates scalability and partial reproducibility but lacks a cohesive, security-by-design template tailored to scientific AI workflows. Our architecture consolidates these concerns.

3. Architectural Design Principles

Modularity & decoupling. Break pipelines into microservices - ingestion, preprocessing, training, inference, visualization - each in an immutable container with a narrow API boundary. Faults are isolated; services evolve independently.

Statelessness & immutability. Keep state in external stores (object stores, databases); treat containers/VMs as immutable artifacts built in CI. Immutability underpins reproducibility (exact digests) and straightforward rollback.

Declarative infrastructure & GitOps. Store Kubernetes manifests/Helm charts/Terraform in Git as the single source of truth. Argo CD (or Flux) continuously reconciles cluster state to Git. Every change is peer-reviewed and auditable, aligning deployment, rollback, and provenance.

Automated CI/CD. Pipelines build signed images, run tests/security scans, and promote artifacts. Deployment gates (policy checks, SAST/DAST/ IaC linting) enforce consistency and reduce drift.

Observability. Metrics (Prometheus), dashboards/alerts (Grafana), logs (ELK/Fluentd), and traces (OpenTelemetry/Jaeger) support performance tuning, debugging, and capacity-aware autoscaling.

Fault tolerance. Replicas, multi-zone node pools, health/readiness probes, and checkpointing enable graceful degradation and resumption of long-running jobs.

Zero-trust security. Enforce least privilege with Kubernetes RBAC and NetworkPolicies; encrypt in transit (mTLS, service mesh) and at rest; manage secrets centrally; scan/sign images; codify policies with OPA/Gatekeeper; monitor at runtime with Falco.

These principles are mutually reinforcing: the same declarative controls that make systems reproducible also reduce attack surface; stateless services enable both autoscaling and reliable restarts; observability informs autoscaling while detecting anomalies.

4. System Design and Implementation

Cluster substrate. A multi-zone Kubernetes cluster orchestrates OCI containers (containerd/CRI-O). An ingress/gateway fronts services; an optional service mesh (e.g., Istio/Linkerd) provides mTLS, traffic management, and telemetry.

Core services.

- Data ingestion. Batch and streaming via Airflow/NiFi and Kafka to decouple producers/consumers. Data lands in a data lake/warehouse (e.g., S3/MinIO, BigQuery) with metadata indexing.
- Preprocessing. Spark for large-scale ETL; Ray for Pythonic, fine-grained parallelism. Orchestrate fan-out/fan-in via Argo Workflows (K8s CRDs). Persist intermediate products with content hashes.
- Training & tracking. Distributed training on CPU/GPU nodes (Spark on K8s, Ray), with MLflow tracking parameters, code versions, metrics, and artifacts. Register models for lineage and promotion.
- Serving. KServe (KFServing) deploys models with autoscaling and canary/blue-green rollouts (via Argo Rollouts). REST/gRPC endpoints expose predictions to scientific clients.
- GitOps & CI/CD. CI builds/scans/signs images and pushes to a registry; Argo CD reconciles live state to Git across dev/stage/prod. Rollback equals git revert.
- Security & policy. OPA/Gatekeeper enforces policies (non-root, resource limits, no host-namespace); registry scanning blocks vulnerable images; Falco alerts on suspicious runtime behavior.

Runtime behavior. HPAs scale stateless services on metrics; Ray/Spark elastic clusters grow and shrink with demand. Pods reschedule on node failure; long-running jobs checkpoint to object storage. All access is authenticated (OIDC/LDAP) and logged.

5. Case Study: $PM_{2.5}$ Air-Quality Forecasting

Goal & data. Forecast hourly $PM_{2.5}$ using OpenAQ measurements and NOAA meteorology. OpenAQ aggregates harmonized air-quality data globally; NOAA provides complementary weather variables.

Pipeline. Hourly collectors push JSON to Kafka; consumers write to a partitioned data lake. Preprocessing removes outliers, imputes gaps, aligns timestamps, and constructs features (lags, temporal encodings, weather joins). Each dataset/version receives a SHA-256 checksum to ensure re-runnability.

Models & training. We train (i) an LSTM in TensorFlow/Keras for temporal dynamics and (ii) an XGBoost regressor as a robust baseline. Training metadata, code commit, container digest, hyperparameters, seeds, input checksums, is logged in MLflow; model artifacts are content-addressed in a registry.

Serving & visualization. The best model is containerized and deployed via KServe. An autoscaled inference API returns 24-hour forecasts; dashboards display predictions, intervals, and recent observations. Access is authenticated; traffic is encrypted.

Evaluation (representative run).

- Ingestion throughput: ~500 records/s average (~40M/day), tolerating bursts via Kafka buffering.
- Preprocessing latency: ~30 s per 100k records with near-linear scaling as worker pods increase.
- Training time: LSTM ~2 h on a 4-node GPU pool (V100 class); XGBoost ~30 min on 16 vCPUs; both reached cross-validated R ≈ 0.80, consistent with prior literature on $PM_{2.5}$ forecasting.
- Inference latency: ~150 ms median per request (p95 ~300 ms); batched multi-city queries ~1.5 s.
- Autoscaling: Load spikes from 10→200 req/s scale replicas 1→5 within ~2 min; CPU stabilizes ~70%.
- Reproducibility: Final cleaned dataset and model binaries recorded with SHA-256 hashes; re-runs produce bitwise-identical artifacts.

These results demonstrate that the blueprint sustains real-time inference while preserving traceability and security.

6. Discussion

Why it works. Reproducibility emerges from immutable artifacts (container digests, dataset checksums), declarative configs (manifests under Git review), and automated rebuild/redeploy pipelines. Scalability follows from stateless microservices, HPAs, and elastic compute pools for data/ML tasks. Security improves through least-privilege defaults, policy-as-code, and runtime monitoring.

Operational considerations.

- Cost/energy: Add carbon-aware scheduling, spot/preemptible nodes, and autoscaling bounds to optimize spend and emissions.
- Hybrid HPC-cloud: Federate identity, share provenance schemas, and package specialized binaries into OCI images to bridge on-prem accelerators and cloud elasticity.
- FAIR data: Enforce metadata standards, lineage-aware retention, and automated PII detection/redaction in CI gates.
- Trustworthy AI: Integrate drift detection, adversarial checks, and model cards into CI/CD as promotion prerequisites.
- Benchmarking: Create suites that couple workload realism with security and reproducibility checks to compare systems beyond throughput alone.

Threat model. Supply-chain attacks (poisoned bases), misconfigurations (over-privileged pods), and lateral movement are primary risks. Image signing/verification, admission control (OPA), SBOMs, and mTLS segmentation mitigate these risks; Falco offers last-mile anomaly detection.

7. Conclusion

We presented a cohesive cloud-native architecture for AI-driven scientific workflows that unifies scalability, reproducibility, and security. By packaging each workflow stage as an immutable, declaratively managed microservice and governing the lifecycle with GitOps and zero-trust controls, research groups can move from brittle scripts to production-grade pipelines. The $PM_{2.5}$ case study demonstrates near-linear scale-out, ~150 ms inference, and bitwise reproducibility, evidence that modern cloud-native practices meaningfully raise both performance and rigor in data-intensive science. Future work will integrate cost/energy modeling, hybrid HPC-cloud federation, FAIR governance automation, and trustworthy-AI gates to further harden and generalize the approach.

References

Ayturan, Y. A., et al. (2020). Short-term prediction of PM2.5 pollution with deep learning methods. NOAA Institutional Repository.

ATLAS Collaboration. (2020). HL-LHC Computing Conceptual Design Report. CERN.

Gutsche, O., et al. (2023). Computing for the High-Luminosity LHC Era. arXiv:2312.00772.

Ivie, P., & Thain, D. (2018). Reproducibility in scientific computing. Computing in Science & Engineering, 20(1), 44–55.

Javed, O., et al. (2021). Understanding the quality of container security scanning tools. arXiv:2101.03844.

Kanwal, S., Khan, F. Z., Lonie, A., & Sinnott, R. O. (2017). Investigating reproducibility and tracking provenance—A genomic workflow case study. BMC Bioinformatics, 18(1), 337. https://doi.org/10.1186/s12859-017-1747-0

Kaur, B., Dugré, M., Hanna, A., & Glatard, T. (2020). An analysis of security vulnerabilities in container images for scientific data analysis. arXiv:2010.13970.

Kubeflow. (n.d.). Kubeflow Pipelines documentation. https://www.kubeflow.org/

KServe. (n.d.). Model serving on Kubernetes. https://kserve.github.io/

MLflow. (n.d.). Tracking, Models, and Registry. https://mlflow.org/

NIST. (2020). Zero Trust Architecture (SP 800-207). https://doi.org/10.6028/NIST.SP.800207

NIST. (2023). A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments (SP 800-207A).

OpenAQ. (n.d.). Platform overview. https://openaq.org/

Pachyderm. (n.d.). Data versioning and lineage for pipelines. https://www.pachyderm.com/

Ray Project. (n.d.). Ray: A unified framework for scaling AI. https://docs.ray.io/

Spark Project. (n.d.). MLlib Guide. https://spark.apache.org/

Argo Workflows & Argo CD. (n.d.). Workflow engine and GitOps for Kubernetes. https://argoproj.github.io/

CNCF. (n.d.). Cloud native definition; Prometheus & Grafana resources. https://www.cncf.io/

Falco Project. (n.d.). Runtime security for containers and Kubernetes. https://falco.org/

M R H Khan(Author) *Emporia State University* **Khalid Aram(Co-Author)**	**Exploring the Association Between Social Media Engagement and Startup VC Funding Outcomes in the Generative AI Sector**

Abstract

This study explores the association between Social Media (SM) engagement and startup funding outcomes in the rapidly expanding Generative Artificial Intelligence (GenAI) sector. Startups rely on digital presence as a key signal to investors, making SM engagement a valuable predictor of Venture Capital (VC) funding. This research analyzes a dataset of 75 GenAI startups to examine the association between SM engagement metrics and funding amounts. Findings reveal that higher SM engagement, as demonstrated through Weighted Engagement Score (WES), is positively associated with funding success in early-stage GenAI startups. Regression analysis suggests that a composite engagement score (WES) derived through Principal Component Analysis

(PCA) demonstrates consistent explanatory power for variance in funding outcomes. WES increases explanatory power (R^2 from 0.37 to 0.43; adjusted R^2 from 0.34 to 0.40) and is positively and significantly associated with funding. This indicates that SM engagement secures VC funding and investor interest in GenAI sector. Further, the study will examine the explanatory power of founder demographics with structural characteristics and WES.

Keywords: Generative AI, social media engagement, startup funding, venture financing, digital entrepreneurship

Introduction

The emergence of Generative Artificial Intelligence (GenAI) startups has created a transformative landscape in entrepreneurial finance and technology (Siddik, Li, & Du, 2024). These ventures operate in an environment characterized by rapid innovation, investor interest, and uncertainty surrounding business models and market acceptance.

For startups in such contexts, access to capital is both essential and challenging. Traditional signals, such as patents, revenue, and partnerships, often lag market entry, making alternative indicators of legitimacy important (Conti et al., 2013; Cheng, 2025). Thus, SM engagement has emerged as an indicator. Platforms such as X (formerly Twitter), Facebook, and LinkedIn serve as primary channels for startups to showcase their innovations, attract users, and establish credibility with investors (Nigam et al., 2020).

Prior research in entrepreneurship has highlighted that visibility and legitimacy influence venture capital (VC) funding decision-making (Pollack et al., 2012; Fischer & Reuber, 2014). However, the specific dynamics of how SM engagement relates to VC funding outcomes in GenAI startups remain underexplored. This study addresses this gap by employing a quantitative exploratory design to analyze the relationship between SM engagement and funding outcomes in GenAI startups. The research aims to provide insights into whether SM engagement signals, such as likes, replies, reposts, and posting frequency of X, are associated with funding success. In doing so, the study contributes to the literature on digital entrepreneurship and venture financing by integrating SM engagement with startup funding success.

Literature Review

Entrepreneurship research has emphasized the importance of signals characterized by information asymmetry between entrepreneurs and investors. Signaling theory suggests that startups communicate quality and legitimacy through observable characteristics, such as patents, strategic alliances, and founder credentials (Spence, 1973; Connelly et al., 2011). SM extends this paradigm by providing continuous, publicly visible signals of activity and credibility. SM has emerged as a powerful platform for entrepreneurs (Kadam & Ayarekar, 2014), influencing various aspects of business operations, networking, investor engagement, and fundraising (Jin et al., 2017; Olanrewaju et al., 2020). Studies suggest that SM engagement enhances a startup's legitimacy by facilitating perceptions of transparency and responsiveness (Fischer & Reuber, 2014; Saxton & Wang, 2014). Engagement metrics such as likes, replies, reposts, and posting frequency serve as proxies for market interest, reinforcing investor confidence.

Nigam et al. (2020) and Abakah et al. (2024) discussed that entrepreneurs with extensive social networks have a higher chance of securing funding from investors and achieving business growth. In the GenAI context, startups face uncertainty due to emerging business models and regulatory scrutiny (Reuel & Undheim, 2024). Here, digital engagement is particularly salient as an early indicator of legitimacy and adoption. While traditional metrics, such as revenue, may take time to materialize, digital signals provide investors with real-time cues about traction. Despite this relevance, limited empirical research has examined the specific relationship between SM engagement and VC financing in GenAI startups, presenting a significant opportunity for exploration.

Methodology

This study employs a quantitative exploratory research design. The dataset consists of GenAI startups that have been active and raised funds between 2020 and 2025, capturing structural characteristics (number of founders, investors, and funding rounds), SM engagement data, and funding amount. We selected X as SM and collected engagement metrics using the X API for 75 startups in the GenAI sector. We applied PCA to engagement metrics to create WES, reducing dimensionality. We used log transformation and standardization of startup data and SM engagement metrics to address skewness, a common practice in PCA and regression modeling (Bayar & Kesici, 2023). We developed the following multiple regression models and examined the relationship between structural variables, WES, and funding outcomes.

- Model 1: $Log(Funding_i) = \beta_0 + \beta_1(Founders_i) + \beta_2(Investors_i) + \beta_3(Rounds_i) + \varepsilon_i$

- Model 2: $Log(Funding_i) = \beta_0 + \beta_1(WES_i) + \beta_2(Founders_i) + \beta_3(Investors_i) + \beta_4(Rounds_i) + \varepsilon_i$

Finally, we interpret the regression results to identify statistically significant predictors of startup funding success. We emphasized the impact of SM engagement, founder characteristics, and funding amount.

Results and Discussion

Findings indicate a consistent positive relationship between SM engagement and startup funding outcomes. Startups with higher levels of engagement, as measured through WES, raise more funding. Model 1, which included only structural characteristics (founders, investors, and funding rounds), is statistically significant overall ($p < .001$). This model explains approximately 37% of the variance in logfunding (Adj.

$R^2 = 0.34$). The number of investors is the strongest positive determinant of funding ($\beta = 0.29$, $p < .001$). Model 2 incorporates the WES with structural variables, remain statistically significant overall ($p < .001$), and demonstrates improved explanatory power (Adj. $R^2 = 0.40$). The model explains 43% of the variance, representing an improvement over Model 1. WES is positively associated with funding ($\beta = 0.18$, $p < .01$). These results provide empirical support for the signaling role of SM engagement in VC financing, particularly within the GenAI sector.

SM engagement plays a role as a form of digital signaling in entrepreneurial finance (Bayar & Kesici, 2023). For GenAI startups, which operate in a rapidly changing environment and with limited historical data, online visibility provides investors with a sense of traction and credibility. The results suggest that GenAI founders should strategically invest in building and maintaining an active SM presence. Regular updates and engagement on X can enhance investor confidence. For investors, monitoring SM engagement may provide an early indicator of promising ventures, complementing traditional due diligence practices. However, this study also underscores the limitations of overreliance on engagement signals. High engagement does not guarantee business viability or a successful revenue model. Investors must balance between digital visibility and evaluating technological and market fundamentals.

Conclusion and Future Work

This study demonstrates that SM engagement is associated with funding outcomes for GenAI startups. WES serves as an important indicator for investors, particularly in early-stage ventures where traditional indicators of success may not be observable. Nevertheless, limitations include reliance on publicly available data and platform-specific biases. Future research should explore the longitudinal effects of SM engagement and differences across SM platforms.

Acknowledgment

The author would like to thank Khalid Aram, Ph.D., CAP-X, for valuable feedback on this manuscript.

References

Abakah, A. A., Kim, G., & Somé, H. Y. (2024). Social networks and start-up funding.

Finance Research Letters, *64*, 105480. https://doi.org/10.1016/j.frl.2024.105480

Bayar, O., & Kesici, E. (2023). The impact of social media on venture capital financing: Evidence from Twitter interactions. *Review of Quantitative Finance and Accounting*, *62*(1), 195–224. https://doi.org/10.1007/s11156-023-01199-4

Cheng, C. (2025). The Role of Digital Social Capital in Startup Funding: A Conceptual

Exploration. *The Transdisciplinary Journal of Management*.

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. Journal of Management, 37(1), 39–67.

https://doi.org/10.1177/0149206310388419

Conti, A., Thursby, J., & Thursby, M. (2013). Patents as signals for startup financing.

Journal of Industrial Economics, 61(3), 592–622. https://doi.org/10.1111/joie.12025

Fischer, E., & Reuber, A. R. (2014). Online entrepreneurial communication: Mitigating

uncertainty and increasing differentiation via Twitter. Journal of Business

Venturing, 29(4), 565–583. https://doi.org/10.1016/j.jbusvent.2014.02.004

Jin, F., Wu, A., & Hitt, L. (2017). Social is the new financial: How startup social media activity influences funding outcomes. *Academy of Management Proceedings, 2017*(1), 13329. https://doi.org/10.5465/ambpp.2017.13329abstract

Kadam, A., & Ayarekar, S. (2014). Impact of Social Media on Entrepreneurship and Entrepreneurial Performance: Special Reference to Small and Medium Scale Enterprises. *SIES Journal of Management, 10*(1).

Nigam, N., Benetti, C., & Johan, S. A. (2020). Digital start-up access to venture capital financing: What signals quality? *Emerging Markets Review*, *45*, 100743. https://doi.org/10.1016/j.ememar.2020.100743

Olanrewaju, A.-S. T., Hossain, M. A., Whiteside, N., & Mercieca, P. (2020). Social Media and Entrepreneurship Research: A literature review. *International Journal of Information Management, 50*, 90–110. https://doi.org/10.1016/j.ijinfomgt.2019.05.011

Pollack, J. M., Rutherford, M. W., & Nagy, B. G. (2012). Preparedness and cognitive legitimacy as antecedents of new venture funding in televised business pitches.

Entrepreneurship Theory and Practice, 36(5), 915–939. https://doi.org/10.1111/j.1540-6520.2012.00531.x

Reuel, A., & Undheim, T. A. (2024). Generative AI needs adaptive governance: The challenge of regulatory uncertainty in emerging AI ecosystems. *arXiv*. https://doi.org/10.48550/arXiv.2406.04554

Saxton, G. D., & Wang, L. (2014). The social network effect: The determinants of giving through social media. Nonprofit and Voluntary Sector Quarterly, 43(5), 850–868. https://doi.org/10.1177/0899764013485159

Siddik, M. N. A., Li, Z., & Du, M. (2024). Unlocking funding success for generative AI startups: The crucial role of investor influence. *Finance Research Letters, 62,* 104091. https://doi.org/10.1016/j.frl.2024.106203

Spence, M. (1973). Job market signaling. The Quarterly Journal of Economics, 87(3), 355–374. https://doi.org/10.2307/1882010

GLOBAL
CONFERENCE ALLIANCE INC.™

Global Conference Alliance Inc.

★★★★★

Please Take a minute & Review Us on Google

CANADA AFRICA INTERNATIONAL BUSINESS CHAMBER OF COMMERCE

ACCREDITED BUSINESS BBB Rating: A+

BC Chamber of Commerce

SBOT SURREY BOARD OF TRADE

40 ANS CCF VANCOUVER

MEMBER OF: The Chamber of Commerce of Metropolitan Montreal

GLOBAL
CONFERENCE ALLIANCE INC.

www.globalconference.ca
contact@globalconference.ca

Contact
+1 236 477 8411 (Customer Service)
+1 672-971-2088 (Hotline & WhatsApp)
Mon to Fri (10 am – 6 pm PST)