International Journal of
Technology and Systems
(IJTS)

Harnessing Emerging Technologies to Construct an Afrocentric Cybersecurity Threat Model

Dr. Joy Kibor

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.11, Issue 1, No.3, pp 35 – 52, 2026

www.iprjb.org

Harnessing Emerging Technologies to Construct an Afrocentric Cybersecurity Threat Model

Dr. Joy Kibor
Lecturer, Zetech University

Article History

Received 14th March 2026

Received in Revised Form 13th April 2026

Accepted 11th May 2026

How to cite in APA format:

Kibor, J. (2026). Harnessing Emerging Technologies to Construct an Afrocentric Cybersecurity Threat Model. *International Journal of Technology and Systems*, *11*(1), 35–52. https://doi.org/10.47604/ijts.3752

Abstract

Purpose: This study examines the rising cybersecurity threats in Africa, where digital transformation particularly mobile money platforms has exposed vulnerabilities such as SIM-swap fraud, USSD attacks, and identity-driven intrusions. Reported losses, including approximately Kshs. 11 billion in Kenya in 2023 and USD 500 million in Nigeria in 2022, underscore the need for contextually relevant cybersecurity strategies. The study proposes an Afrocentric approach integrating Artificial Intelligence (AI), Big Data, and Cloud Computing to enhance threat detection, intelligence sharing, and adaptive defense mechanisms.

Methodology: A Systematic Literature Review (SLR) guided by PRISMA principles was conducted, examining peer-reviewed studies, industry reports, and policy documents from 2020 to 2025 across IEEE Xplore, Scopus, ScienceDirect, and SpringerLink. The review focused on African cybersecurity challenges, applications of emerging technologies, and culturally relevant digital governance frameworks. Thematic synthesis identified gaps and informed the development of a conceptual Afrocentric cybersecurity model.

Findings: Current Western-centric frameworks inadequately address Africa's mobile-first digital ecosystem. The proposed Afrocentric model integrates AI-driven analysis of mobile transactions, Big Data analytics for real-time threat intelligence, and cloud infrastructure designed for localized data governance. The framework embeds collective intelligence sharing inspired by Ubuntu philosophy and emphasizes Managed Shared Responsibility to overcome technical literacy gaps in SMEs.

Unique Contribution to Theory, Practice and Policy: African governments, industry, and policymakers should adopt Afrocentric cybersecurity strategies prioritizing mobile ecosystems, develop local AI and Big Data capacity, and establish secure cloud infrastructures. Future research should empirically test the model to strengthen digital resilience across African economies.

Keywords: *Afrocentric Cybersecurity, Artificial Intelligence, Big Data, Cloud Computing, Mobile Money, SIM-Swap Fraud, USSD Vulnerabilities, Africa, 4IR*

JEL Classification: *O33, L86, C88, D83*

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.11, Issue 1, No.3, pp 35 – 52, 2026
www.iprjb.org

INTRODUCTION

This research examines the rapidly evolving cybersecurity landscape, with a focus on the potential of Artificial Intelligence (AI), Big Data, and Cloud Computing to inform a contextually grounded, yet globally adaptable, framework for mitigating cyber threats. While the study emphasizes African realities, the conceptual model is designed to be applicable beyond the continent, informed by socio-technical characteristics such as communal data-sharing practices, mobile-first architectures, and high-density "closed" social networks that are common in African societies. The expansion of digital technologies across Africa introduces tremendous opportunities for socio-economic development; however, it has also created a fertile environment for increasingly sophisticated and organized cyberattacks.

Recent estimates indicate that African economies continue to bear massive losses due to cybercrime, amounting to billions of dollars annually (African Union, 2025). Alarmingly, AI-driven phishing schemes and identity-based intrusions now account for nearly 48% of regional cybersecurity incidents (International Telecommunication Union. 2025). With growing internet penetration, widespread adoption of mobile and cloud services, and a surge in digital transactions, vulnerabilities are escalating at unprecedented speed. Addressing these challenges requires more than technical solutions; it calls for comprehensive, dynamic, and culturally relevant cybersecurity strategies.

Traditional cybersecurity frameworks, often developed in Western contexts, fail to adequately reflect Africa's socio-economic, cultural, and infrastructural realities. These models often overlook unique governance structures, linguistic diversity, locally perceived threat types, and informal knowledge networks. Over-reliance on imported technologies, low digital literacy, and a shortage of cybersecurity expertise further widen the protection gap (Msukwa & Dlodlo, 2021). In response, there is a growing call for African-led models that localize technology application and reframe cybersecurity in culturally sustainable ways.

This study proposes the development of an Afrocentric cybersecurity model; a conceptual framework anchored in African socio-technical realities yet adaptable to other regions. The model leverages the transformative capabilities of AI, Big Data, and Cloud Computing to deliver scalable, real-time, and forward-looking cybersecurity solutions. AI facilitates real-time threat detection, behavioral anomaly identification, and automated response, making it indispensable against increasingly sophisticated attacks (IBM, 2025). Big Data analytics processes vast, heterogeneous datasets to detect threat patterns, predict vulnerabilities, and inform evidence-based responses. Cloud Computing provides cost-effective, flexible infrastructure essential for deploying AI- and data-driven cybersecurity solutions, particularly in resource-constrained environments (Cisco, 2024).

Despite global attention to cybersecurity, most existing models remain generic and insufficiently attuned to African socio-technical realities. The knowledge gap is evident in the limited integration of local governance structures, indigenous epistemologies, communal data-sharing practices, and region-specific threat landscapes. As cyber threats become increasingly transnational, Africa and by extension, other regions with similar socio-technical configurations risks being targeted unless strategies evolve to match the speed, scale, and complexity of these threats.

Cybersecurity has therefore emerged as a critical issue of national security, economic resilience, and digital sovereignty. Inadequate digital defenses can disrupt essential services, compromise governance, jeopardize citizen data, and erode public trust. An Afrocentric model provides a timely recalibration, aligning cybersecurity strategies with African developmental goals, promoting regional cooperation, and fostering digital self-reliance. This paper conceptualizes and proposes such a model, integrating AI, Big Data, and Cloud Computing as foundational pillars, thereby addressing the dual imperative of technological innovation and contextual relevance in African and globally informed cybersecurity discourse.

LITERATURE REVIEW

Cybersecurity Challenges in Africa and the Need for Contextual Solutions

African nations are increasingly confronting cybersecurity challenges that are not only technical but also socio-political in nature. Much of the existing cybersecurity infrastructure and frameworks in Africa remain Western-centric, reflecting technological paradigms, assumptions, and priorities developed in contexts vastly different from those of African countries. This reliance on imported solutions has been described as a form of "digital colonialism", where technology adoption fosters technological dependency rather than building local capacities and resilience (Ezekwueme & Sunday, 2025). Consequently, these models may inadequately address Africa's unique socio-technical realities, including communal data-sharing practices, mobile-first architectures, and high-density "closed" social networks.

The intersection of Artificial Intelligence (AI), Big Data, and Cloud Computing offers immense potential to transform cybersecurity, yet its application within an Afrocentric framework remains underexplored. Existing literature often highlights the general benefits of these technologies or discusses African cybersecurity challenges in isolation, leaving a critical gap for approaches that integrate local realities with advanced technological tools. This review synthesizes relevant research from the last five years, highlighting interconnected themes and identifying areas that necessitate an Afrocentric approach.

Recent reports consistently underscore the escalating cybersecurity threats faced by African nations. Interpol's African Cyberthreat Assessment Report 2025 points to a rising incidence of cyberattacks targeting critical infrastructure, financial institutions, and individuals across the continent, attributing this surge to increased reliance on digital services coupled with insufficient security measures (Interpol, 2025). Similarly, the African Union (AU) acknowledges that rapid digital transformation is outpacing the development of robust cybersecurity laws and regulations, resulting in significant vulnerabilities (African Union, 2024).

Several studies emphasize the limitations of Western-centric frameworks in the African context. Msukwa and Dlodlo (2021) argue that traditional models often overlook indigenous knowledge systems and fail to account for the resource constraints typical in developing economies. They stress the importance of contextually relevant solutions. The African Cyber Programme further notes that countries like Kenya are actively developing national cybersecurity strategies; however, the effectiveness of these strategies can be enhanced by incorporating local realities and fostering public-private partnerships (KPMG, 2023). Collectively, these works underscore the necessity for

tailored, Afrocentric cybersecurity approaches that not only leverage emerging technologies but also respond to Africa's distinct socio-technical and regulatory environment.

The Role of Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) has become a cornerstone of modern cybersecurity, offering transformative capabilities that extend beyond traditional, signature-based approaches. In African contexts, AI's potential is particularly significant due to the increasing volume and sophistication of cyber threats, coupled with diverse socio-technical realities. Research consistently demonstrates that AI can enhance real-time threat detection, recognize anomalies, identify zero-day exploits, and detect insider threats by processing large volumes of security data efficiently (IBM, 2025; Hussain & Alqahtani, 2021). Machine learning algorithms, in particular, allow security systems to analyze complex patterns, prioritize threats, and generate actionable recommendations for security professionals. The African Union's Continental Artificial Intelligence Strategy emphasizes the importance of leveraging AI responsibly, highlighting its potential to support localized threat intelligence while addressing risks such as bias, ethical dilemmas, and the inclusion of indigenous knowledge (African Union, 2025). Together, these capabilities make AI an indispensable tool for building proactive, predictive, and adaptive cybersecurity frameworks that can respond to Africa's unique threat landscape.

Despite its transformative benefits, the deployment of AI in cybersecurity raises several critical challenges, particularly when developing an Afrocentric model. A primary concern is the quality and representativeness of training data, as AI models rely on large datasets to function effectively, and incomplete or biased data can produce skewed outcomes and exacerbate existing inequalities (Palo Alto Networks, 2025.; Hussain, & Alqahtani, 2021). Additionally, the "black box" nature of certain AI algorithms creates transparency and interpretability issues, complicating accountability and trust in critical security decisions (MITRE. 2023). The dual-use potential of AI further compounds these challenges, with malicious actors leveraging AI to automate phishing campaigns, generate deepfakes, and deploy adaptive malware (McKinsey, 2025). In African contexts, where digital infrastructures are often resource-constrained and data landscapes are highly diverse, these issues underscore the necessity for contextually informed, ethical, and human-supervised AI deployment. Effective integration of AI must therefore include considerations of data governance, bias mitigation, local data diversity, and human oversight, ensuring equitable security outcomes while strengthening regional digital resilience (African Union, 2025; Msukwa & Dlodlo, 2021).

Leveraging Big Data for Enhanced Cybersecurity Intelligence

The scale, complexity, and velocity of cybersecurity-related data in Africa necessitate robust Big Data analytics to support effective threat intelligence. Unlike traditional environments, African digital ecosystems are heavily shaped by the widespread adoption of Mobile Money platforms and other FinTech solutions, which generate enormous volumes of real-time transactional, behavioral, and financial data. These datasets, encompassing network activity, payment records, and user interactions, provide a unique opportunity for predictive cybersecurity, enabling the identification of anomalies, fraudulent patterns, and emerging threats before they escalate into large-scale incidents (Akinyemi, et al., 2020; Chen, et al.,2021).

The contemporary cybersecurity landscape has also entered what is often referred to as the "Agentic Era" of AI, where data pipelines are no longer passive repositories but autonomous systems capable of real-time analysis, decision-making, and automated threat response. In this context, Big Data security extends beyond traditional storage protections to include safeguarding the integrity and reliability of AI-driven workflows. For Africa, this means that FinTech transaction streams and other high-frequency data sources must be secured not only at rest but throughout dynamic, self-learning pipelines that continuously adapt to evolving threats. Properly managed, these pipelines allow organizations to detect and respond to anomalies in milliseconds, a critical capability given the speed and sophistication of cyber-attacks targeting mobile payment infrastructures and cloud-based financial services (Hussain & Alqahtani, 2021; IBM Security, 2025).

Despite its transformative potential, leveraging Big Data in Africa faces distinct challenges. Infrastructure limitations, inconsistent data governance, and scarcity of skilled personnel capable of handling advanced analytics can constrain the effective deployment of predictive cybersecurity models (Msukwa & Dlodlo, 2021). Furthermore, the sensitive nature of financial and personal data necessitates stringent privacy measures, compliance with emerging African cybersecurity regulations, and integration of ethical considerations into data collection and analysis practices. An Afrocentric model must therefore prioritize building resilient local data ecosystems, enhance human capacity through targeted training, and implement governance frameworks that secure both the datasets and the autonomous AI-driven systems that analyze them (Akinyemi et al., 2020; African Union, 2025).

Therefore, Big Data analytics provides a powerful mechanism for predictive, proactive, and contextually relevant cybersecurity in Africa, particularly when applied to FinTech and mobile-first environments. Thus, by combining large-scale data processing with autonomous AI-driven analysis, an Afrocentric approach can transform the region's cybersecurity posture, enabling organizations to detect threats earlier, respond faster, and build sustainable, locally grounded intelligence systems capable of evolving with emerging challenges.

Cloud Computing as an Enabler for African Cybersecurity

Cloud computing has become a central pillar of digital transformation in Africa, enabling organizations to access scalable infrastructure, reduce capital expenditure, and deploy advanced digital services without heavy investment in on-premises systems. For cybersecurity, cloud environments provide continuous security updates, centralized monitoring, and access to enterprise-grade protections such as distributed denial-of-service (DDoS) mitigation, encryption services, and global threat intelligence systems (Cisco, 2024). These capabilities are particularly valuable in African contexts where many public institutions and SMEs face resource constraints yet remain increasingly dependent on digital platforms for service delivery and financial transactions.

Beyond its benefits, cloud adoption introduces complex security governance challenges. Key concerns include data sovereignty, cross-border data flows, regulatory fragmentation, and uneven compliance with emerging African data protection frameworks. Additionally, infrastructural disparities such as unreliable connectivity, inconsistent power supply, and limited cloud security expertise continue to affect the secure deployment and management of cloud services across the

continent (OECD, 2023). These limitations complicate the effective implementation of the standard shared responsibility model, which assumes that cloud users possess sufficient technical capacity to configure and manage their security obligations.

In practice, particularly among African SMEs, the shared responsibility model often degenerates into a form of "de facto no responsibility", where users lack the technical literacy to secure applications, access controls, and configurations, thereby leaving critical security gaps unaddressed. This creates an urgent need to rethink cloud governance models in a way that reflects local capacity realities.

To address this, an Afrocentric cloud security approach should adopt a Managed Shared Responsibility Model, where local cloud service providers, managed security partners, and regional data centres take a more active role in configuring, monitoring, and securing cloud environments for SMEs and public institutions. This model shifts responsibility from purely end-user control to a collaborative security ecosystem, ensuring continuous support, compliance enforcement, and contextual alignment with African regulatory and infrastructural realities. Emerging African cloud infrastructure initiatives, including regional data centres operated by providers such as Liquid Intelligent Technologies, demonstrate the feasibility of such localized cloud governance ecosystems (World Bank, 2022; African Union, 2024).

By embedding cloud computing within a context-sensitive governance framework, Africa can transform cloud adoption from a potential vulnerability into a strategic cybersecurity asset that strengthens digital resilience, supports economic growth, and enhances regional technological sovereignty.

Towards an Afrocentric Integration

Although existing studies have independently explored Artificial Intelligence, Big Data, and Cloud Computing in cybersecurity, and others have highlighted Africa's cybersecurity challenges, there remains a notable absence of a fully integrated Afrocentric cybersecurity model. Most existing frameworks are still largely shaped by Western epistemologies, with limited consideration of African socio-cultural realities, indigenous knowledge systems, and the broader pursuit of digital self-determination. While the African Union's vision of an "Africa-centric, development-oriented and inclusive approach" to emerging technologies provides an important policy foundation (African Union, 2024), its practical translation into an integrated cybersecurity architecture that combines AI, Big Data, and Cloud Computing remains underdeveloped.

Towards an Afrocentric integration therefore represents a deliberate epistemological and technological shift away from imported, individualistic cybersecurity paradigms toward a framework grounded in African social realities, values, and collective worldviews. Central to this shift is the Ubuntu philosophy, which emphasizes that "I am because we are," reflecting a deeply communal understanding of identity, responsibility, and wellbeing. In digital terms, Ubuntu supports a cybersecurity paradigm where threat intelligence is shared collectively rather than siloed, enabling organizations, governments, and individuals to participate in crowdsourced cyber defense ecosystems. This contrasts sharply with dominant Western models, which prioritize individual data ownership and highly fragmented threat visibility. In African socio-digital environments characterized by communal networks, mobile-first communication systems, and

shared digital infrastructures Ubuntu-aligned cybersecurity systems are more contextually appropriate and operationally effective.

Within this framework, AI and Big Data systems must be designed to support collective threat intelligence sharing, enabling real-time aggregation of cyber incidents across institutions, mobile money platforms, and cloud environments. Such an approach improves early warning systems, enhances anomaly detection, and strengthens coordinated responses to rapidly evolving threats such as mobile money fraud and identity-based attacks, which are increasingly prevalent in African digital ecosystems (African Union, 2024; Tremhost, 2025). However, this must be balanced with ethical data governance frameworks that respect privacy while still enabling controlled communal intelligence sharing.

In addition, Afrocentric integration requires robust attention to data sovereignty and infrastructural independence. The establishment of localized cloud infrastructure and regional data centres is essential to reduce over-reliance on external providers while ensuring compliance with African regulatory frameworks and cultural expectations regarding data stewardship (CIO Africa, 2025; Interpol, 2025). Such infrastructure also strengthens trust in shared cybersecurity ecosystems by ensuring that data used for collective threat intelligence remains under appropriate regional governance.

A further pillar of this integration is the development of indigenous cybersecurity capacity and digital self-determination. This involves significant investment in culturally responsive education, skills development, and research ecosystems that position Africans not only as consumers of cybersecurity technologies but also as active producers of AI-driven security solutions (Msukwa & Dlodlo, 2021; World Economic Forum, 2025). In this way, Afrocentric cybersecurity becomes both a technical and developmental agenda.

The proposed model therefore aligns with the principles of Afrocentricity (Asante, 1987), emphasizing African agency, epistemological autonomy, and contextual relevance in digital security systems. It also recognizes the heterogeneity of digital maturity across the continent, advocating for flexible, scalable, and locally adaptive solutions rather than one-size-fits-all frameworks. Its alignment with continental initiatives such as the AU Digital Transformation Strategy (2020–2030) and the Smart Africa Blueprint further reinforces its policy relevance and implementation potential.

Ultimately, achieving this transformation requires a multi-stakeholder ecosystem involving governments, academia, private sector actors, and civil society, working collaboratively to co-create cybersecurity systems that are ethically grounded, technologically advanced, and contextually relevant. The integration of Ubuntu philosophy into cybersecurity thus reframes digital security as a shared societal responsibility rather than an individual or institutional function, enabling a more resilient, inclusive, and adaptive African cyberspace.

The absence of such an integrated framework in existing literature underscores the significance of this study. By combining Afrocentric principles, Ubuntu philosophy, and emerging technologies such as AI, Big Data, and Cloud Computing, this research contributes toward the development of a contextually grounded cybersecurity model that enhances digital resilience while restoring African agency in the governance of cyberspace.

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.11, Issue 1, No.3, pp 35 – 52, 2026
www.iprjb.org

Cybersecurity Threats

The modern cybersecurity landscape is increasingly complex, driven by rapid technological innovation and the evolving sophistication of cybercriminal activity. Globally, cybercrime has escalated in both scale and impact, with the latest industry reports estimating that financial losses from cybercrime will reach $10.5 trillion by 2025 (Cybersecurity Ventures, 2025). Advanced persistent threats, ransomware, and AI-enhanced phishing attacks continue to dominate globally, targeting critical infrastructure, financial systems, and personal data (Interpol, 2025; Cisco, 2025). The proliferation of AI-driven tools has made both the execution and detection of cyberattacks more dynamic, requiring responsive, automated, and predictive cybersecurity measures.

In Africa, the cybersecurity threat landscape presents unique characteristics that distinguish it from Western contexts. While traditional cyber threats such as ransomware, malware, and phishing exist, a substantial portion of attacks in the region target mobile-first financial systems, including Mobile Money platforms such as M-Pesa, MTN MoMo, and Airtel Money. The widespread adoption of mobile payments, agent-based transaction networks, and USSD-driven interfaces has created new vulnerabilities. For instance, SIM-swap fraud, unauthorized USSD session exploitation, and agent network compromise have emerged as dominant attack vectors, often resulting in significant financial losses for individuals and organizations (Tremhost, 2025; Kearney, 2024). AI-driven social engineering scams, particularly through WhatsApp and other mobile messaging applications, now account for a growing percentage of these fraud incidents, highlighting the importance of integrating intelligent threat detection mechanisms in local cybersecurity frameworks (McKinsey, 2025).

African organizations also contend with resource constraints, including limited cybersecurity budgets, shortage of skilled personnel, and inconsistent regulatory frameworks (Msukwa & Dlodlo, 2021). These challenges exacerbate the continent's vulnerability to both conventional and emerging threats, including supply-chain attacks, critical infrastructure intrusions, and fraud targeting financial institutions (World Economic Forum, 2025; Interpol, 2025). Additionally, legacy hardware and software, coupled with uneven internet connectivity, increase exposure to cyber threats, particularly in rural and semi-urban areas where mobile money usage is prevalent.

AI is increasingly employed to counter these threats, enabling real-time monitoring, anomaly detection, and automated incident response. Machine learning models can identify suspicious patterns in transaction data, detect fraudulent agent activities, and mitigate identity-based intrusions (IBM, 2025). However, African cybersecurity initiatives must also contend with dual-use challenges, where AI itself can be exploited by attackers to automate phishing, deepfake scams, and mobile wallet fraud campaigns. This underscores the need for AI systems trained on local datasets that reflect African transaction patterns, behavioral norms, and fraud tactics to ensure effective detection and equitable protection (African Union, 2024).

An Afrocentric approach to cybersecurity in Africa, therefore, must prioritize contextual threat mitigation. Mobile Money systems should be treated as the primary attack surface, with interventions tailored to USSD, SIM-swap, and agent-based vulnerabilities. Threat intelligence sharing, crowdsourced through communal networks in line with Ubuntu-inspired principles, can enhance early detection and collective defense mechanisms, creating a more resilient and culturally aligned cybersecurity ecosystem. By focusing on local realities rather than imported, Western-

centric frameworks, such a model would allow African nations to safeguard digital financial services, critical infrastructure, and citizen data in a manner that is both technologically sophisticated and socially relevant.

Artificial Intelligence

Artificial Intelligence is now a buzz word in both technical and non-technical circles. The growth in this area is phenomenal. The many applications that AI has been able to front are astonishing to the tech industry. The exponential growth of Artificial Intelligence (AI) adoption in Africa heralds a transformative era, where technological innovations are becoming instrumental in tackling pressing socio-economic challenges and driving developmental initiatives, Santosh and Gaur, (2022). In 2017, Price Waterhouse Coopers released a report forecasting a substantial contribution of US$15.7 trillion to the global economy by 2030, (Rao & Verweij, 2017). However, the distribution of wealth and influence derived from AI technologies has been notably uneven. PWC's depiction of the future AI-driven economy, as illustrated below, highlights minimal growth for the African continent. Despite this, Africa plays a pivotal role in the development of AI systems, contributing natural resources, labor, and skills from across the region. Despite the extensive global reach of the AI supply chain, the advantages of these technologies have yet to materialize in Africa. Instead, they predominantly benefit Big Tech companies in the Global North and China, along with those who can afford the daily conveniences offered by AI through devices like Amazon's Alexa and smart cars, (Kinyua & Kute, 2023).

Recently, more than 1000 AI enthusiasts from more than 95 countries converged on Kigali for the first-ever Global AI Summit on Africa. Organized by the World Economic Forum, which estimates the continent will get a miserly $2.9 trillion from the $19.9 trillion AI will generate by 2030, keynote speakers included Rwandan President Paul Kagame and his Togolese counterpart Faure Gnassingbé. Kagame called for investment and commitment. "Our strategy should be to go back to the drawing board and build a stronger foundation for connectivity," he urged delegates at the summit. "Africa cannot afford to be left behind, once again, playing catch-up", Ekonde, (2025).

Since 2022, when OpenAI rolled out ChatGPT and marked the turning point for AI, ushering in global adoption that has led to groundbreaking innovation and giant investments, there have been concerns that Africa will be left behind. Since the onset of industrialization in the 1800s, Africa has been playing catch-up due to myriad barriers, many of them intentionally imposed and maintained through colonial and post-colonial administration. In the advent of AI, Africa is still to get up to speed, (Ekonde, 2025).

Following the two-day summit, participants pledged to establish a $60 billion fund an amount nearly equivalent to Uganda's total GDP in 2024, making it comparable to the output of Africa's 13th-largest economy. According to the summit's declaration, the fund will be used to strengthen AI infrastructure, support African startups and machine learning innovators, and promote the localization of AI research across the continent.

Strive Masiyiwa, the Zimbabwean entrepreneur and head of Cassava Technologies the company behind Africa's first AI factory told delegates that his company is set to receive the first 3,000 units of the technology in May. These units will be installed at Cassava's data center in South Africa by

June. An additional 7,000 units are scheduled for deployment across Kenya, Nigeria, Morocco, and Egypt (Ekonde, 2025).

Artificial Intelligence happens when large datasets are collected, computed, and trained by using step-by-step processes (algorithms) aimed at solving problems or performing tasks. This requires graphic processing units (GPUs) that can perform quadrillions of calculations and functions within seconds. Nvidia, the American chipmaker, produces 85% of the GPUs that do the work. Alex Tsado, co-founder of Alliance4AI, an organization that rallies African AI engineers, told CNN that innovators' access to the supercomputers will turbocharge computing power on the continent. Computer scientists will be encouraged to collect more data because they will be able to transform it, and there will be broad machine learning programs, he said, Ekonde, (2025).

Three key areas stand out as having significant potential for AI in retail industry, (Oosthuizen, et. al., 2021). First, personalized design and production hold promise for a future where products can be tailored to individual preferences and needs. Retailers are increasingly leveraging deep learning to anticipate customer demand, predicting orders in advance. This not only streamlines inventory and delivery management but also aligns with the consumer benefit of on-demand customization, offering greater availability of desired products. In terms of timing, product recommendations based on preferences are already a reality, while the medium-term potential includes fully customized products. In the longer term, AI-driven products may anticipate market demand signals. The time saved for consumers is notable, as AI eliminates the need to extensively explore shelves, catalogues, or websites. However, barriers to overcome include adapting design and production to this agile and tailored approach, along with the imperative for businesses to bolster trust regarding data usage and protection. A high-potential use case is personalized design and production, particularly in sectors like fashion, where AI could facilitate interactive and customized design and supply processes based on user feedback, Kinyua & Kute, (2023).

Big Data

Every key stroke generates data as countries around the globe forge ahead on their digital transformation journeys, the amount of data being generated is staggering. In the right hands and used responsibly, this data represents limitless opportunities for growth and digital advancement. In the wrong hands, it exposes individuals and organizations to levels of cybercrime that have the potential to cause untold financial and data losses, even crippling businesses. Recent market research reports that the global big data market is set to grow from USD 138.9 billion in 2020 to USD 229.4 billion by 2025, due in part to the escalating demand for data-driven decision-making by organizations looking to gain a competitive advantage, (*De Villiers,* 2024).

Big data analytics will be a must-have component of any effective cyber security solution due to the need of fast processing of the high-velocity, high-volume data from various sources to discover anomalies and/or attack patterns as fast as possible to limit the vulnerability of the systems and increase their resilience. Even though many big data analytics tools have been developed in the past few years, their usage in the field of cyber security warrants new approaches considering many aspects including (a) unified data representation, (b) zero-day attack detection, (c) data sharing across threat detection systems, (d) real time analysis, (e) sampling and dimensionality reduction, (f) resource-constrained data processing, and (g) time series analysis for anomaly detection, (Angin, 2019).

This has been the case with the era of Internet of Things which has billions of smart devices connected to the internet making the surface of potential attacks easier and bigger to target by cyber attackers, leading to the necessity of quick and accurate detection of such attack. In the last ten years, advances in mobile computing, communications and mass storage architecture have led to the phenomenon known in the world as big data that is characterized by unprecedented large volume of useful data being created in various formats and at a very elevated pace. This capability to process these huge volumes of data in real time through big data analytics tool comes with many advantages that can be applied in cyber threat analysis systems. With the help of the big data gathered by networks, computers, sensors, and cloud systems, the cyber threat analyst and the intrusion detection/prevention system will be in a position of finding valuable information in real time. Such information could assist in identifying possible system weak points and attacks that are increasing and establishing security mechanisms against them, (Angin, 2019).

Cloud Computing

Cloud computing has developed as an all-transforming innovation, disrupting how organizations save, deal with, and gain access to information. Cloud computing is gaining popularity in Africa as digital transformation is needed, and efficiency and scalability will be achieved. Nonetheless, the extent of cyberattacks is also growing with the number of clouds used which introduces great risks in the stability and safety of the cloud-hosted structures. In this literature paper, the researcher will expose the advancements in safeguarding cloud computing in Africa against cyber security threats. It is premised on an in-depth review of peer-to-peer research and surveys, market reports, and policy publications. The article begins with basic analysis of cloud computing touching on its key characteristics and benefits such as being affordable, expandable as well as flexible, (Armbrust, 2010). It can be found in the essay in which the specific context of the adoption of the cloud computing will be discussed, where the factors are examined that lead to its acceptance and the ones which hinder its wide implementation in Africa. (Mbuyu, 2021).

The literature further highlights the prevailing cyber threats targeting cloud infrastructure in Africa, including data breaches, ransomware attacks, and insider threats (Kumar & Singh, 2020). To address these challenges, recent advancements in cloud cybersecurity are examined. These include the adoption of advanced encryption techniques, the implementation of zero-trust security architectures, and the integration of artificial intelligence (AI) to enhance threat detection and response capabilities (Ezugwu, 2021). UNCTAD, 2021 emphasizes the significance of international cooperation and capacity-building activities in enhancing cybersecurity frameworks in Africa.

There have been enhancements in security measures for cloud computing. The latest developments in cybersecurity technologies play a crucial role in strengthening cloud infrastructure against ever-changing cyber-attacks (Ezugwu, 2021). “Encryption methods, such as homomorphic encryption and quantum-resistant cryptography, are crucial for protecting the secrecy and integrity of data while it is being sent and while it is at rest”, (Zissis & Lekkas, 2012). “Moreover, the implementation of zero-trust security architectures highlights the significance of ongoing verification and detailed access restrictions to reduce the risks posed by insiders and restrict the mobility inside cloud environments”, says, Kumar and Singh, (2020). “By utilizing artificial intelligence (AI) and machine learning (ML) algorithms, businesses may increase their ability to

detect threats, automate incident response, and boost their overall security position, says, (Le, 2020).

Cloud computing has rapidly evolved from a novel concept to a foundational pillar of modern IT infrastructure, offering significant benefits in scalability, cost-efficiency, and flexibility. Its "pay-as-you-go" model and on-demand resource provisioning make it particularly attractive for organizations, including those in developing economies, seeking to modernize their digital capabilities without substantial upfront capital expenditure (Kaopiz, 2025). Such benefits include centralized security management, automated updates, and strong security postures typically held by large cloud service providers (CSPs), which may exceed those of most separate organizations, in the realm of cybersecurity (IBM,2025). Such advantages are of paramount importance to African countries, as it will allow tapping into advanced cybersecurity means and facilities that would not be affordable or technically feasible because of the cost (CIO Africa, 2025a).

Although these arguments make adoption of cloud computing very attractive, there are issues and security considerations that would discourage adoption of cloud computing in Africa especially with regard to sensitive data and critical infrastructure in the government. Indeed, the research notes that issues such as the sovereignty of data, compliance with regulations, and the availability and stability of the internet and power are too often barriers to the continent (Msukwa & Dlodlo, 2021; Tremhost, 2025). Misunderstanding of the shared responsibility model in cloud security where CSPs protect only infrastructure underlying their cloud but clients are in charge of their data and access controls usually results in a security breach (African Union, 2025). In addition, although cloud environments have, as standard, superb security solutions, they present new vectors of attack as well, such as insecure APIs, account compromises, and internal users, requiring the introduction of powerful identity and access management (IAM) and monitoring (Cisco,2024). As such, an effective integration of cloud computing technology in cybersecurity needs to take these risks seriously beforehand by pursuing location-specific data control, trust by demonstrating openness, and regional cloud skills to make solutions not only technologically advanced but also locally secure.

METHODOLOGY

This study employed a Systematic Literature Review (SLR) to critically synthesize existing scholarly and industry knowledge on Artificial Intelligence, Big Data, and Cloud Computing in relation to cybersecurity threats, with the aim of informing the development of an Afrocentric cybersecurity model. The SLR approach was deemed appropriate because it enables a structured, transparent, and reproducible examination of existing literature, allowing for the identification of patterns, gaps, and emerging conceptual directions without the need for primary data collection. The review followed established principles aligned with the PRISMA framework to enhance methodological rigor, transparency, and replicability.

The literature search was conducted across multiple reputable academic databases to ensure comprehensive coverage of peer-reviewed and high-quality sources. These databases included IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, Scopus, ACM Digital Library, and Web of Science, with Google Scholar used as a supplementary search engine to capture additional relevant studies and grey literature from credible institutional sources. The search strategy was guided by carefully constructed keyword combinations such as “Artificial Intelligence AND cybersecurity

AND Africa," "Big Data analytics AND cyber threats," "Cloud computing security AND developing economies," "Afrocentric cybersecurity model," and "mobile money fraud AND cybersecurity Africa." Boolean operators (AND/OR) were applied to refine and expand the search results, ensuring both specificity and breadth in capturing relevant studies.

To maintain relevance and currency, the search was limited to publications between 2020 and 2025, reflecting the most recent developments in cybersecurity, artificial intelligence, and digital infrastructure, particularly within African and comparable developing contexts. Only peer-reviewed journal articles, conference papers, and credible institutional or industry reports were considered. Studies were included if they addressed at least one of the core constructs Artificial Intelligence, Big Data, Cloud Computing, or cybersecurity and provided empirical, conceptual, or policy-relevant insights applicable to African or similar socio-technical environments. In addition, studies were required to be published in English to ensure accessibility and consistency in analysis.

The exclusion criteria eliminated non-peer-reviewed materials such as blogs, opinion articles, and informal commentaries, as well as duplicate records, studies published before 2020, and works that lacked clear methodological or conceptual grounding. Studies that were not directly relevant to cybersecurity or digital technologies were also excluded to maintain focus and analytical precision.

Following the search and retrieval process, all identified studies were imported into a reference management system, where duplicates were removed. The remaining studies underwent a two-stage screening process involving title and abstract review, followed by full-text assessment against the inclusion criteria. This systematic screening ensured that only studies meeting the required relevance and quality thresholds were included in the final synthesis.

Data extracted from the selected studies focused on cybersecurity threat patterns, applications of Artificial Intelligence, Big Data, and Cloud Computing in security environments, as well as Africa-specific digital ecosystem characteristics such as mobile money systems, FinTech platforms, and infrastructural constraints. A thematic synthesis approach was then applied to integrate findings across studies, enabling the identification of recurring themes, contradictions, and conceptual gaps in the literature. These synthesized insights formed the foundation for the development of the proposed Afrocentric cybersecurity model.

Discussion

The systematic literature review conducted for this study provides critical insights into the evolving cybersecurity landscape in Africa, particularly highlighting the persistent gaps in contextually responsive frameworks. The continent's rapid digital transformation, while offering significant socio-economic opportunities, has simultaneously increased exposure to sophisticated cyber threats. These threats are amplified by structural vulnerabilities such as limited digital infrastructure, skill shortages, fragmented regulatory frameworks, and reliance on imported cybersecurity solutions (Interpol, 2025; World Economic Forum, 2025). In particular, Africa's mobile-first economy, reliance on USSD and SMS-based transactions, and rapidly expanding FinTech ecosystems create threat vectors that Western-centric models often overlook.

Our review underscores that prevailing cybersecurity frameworks, largely rooted in Western paradigms, are insufficient for addressing African realities. Western models primarily focus on

high-bandwidth enterprise networks, cloud infrastructures, and web-based attacks, often disregarding low-bandwidth mobile transactions, agent-based banking networks, and localized fraud patterns. In African contexts, cyber threats frequently exploit these overlooked channels, including mobile money fraud, SIM-swap attacks, and phishing through SMS or USSD channels. An Afrocentric approach, therefore, requires a paradigm shift that integrates technological sophistication with cultural, economic, and infrastructural specificities of African societies (Msukwa & Dlodlo, 2021).

The review confirms the transformative potential of AI, Big Data, and Cloud Computing in enhancing cybersecurity resilience in Africa. Specifically, AI can be harnessed to analyze USSD and SMS-based transaction patterns, identifying anomalies indicative of SIM-swap fraud, fraudulent agent behavior, or phishing attempts targeting mobile money users. Such AI-driven insights extend beyond traditional signature-based threat detection, enabling predictive monitoring and rapid mitigation of risks in real time. By training machine learning algorithms on African transaction datasets, bias introduced by Western data distributions can be mitigated, improving predictive accuracy and fairness within local digital ecosystems (IBM, 2023; Tremhost, 2025). Moreover, AI's capacity for behavioral modeling facilitates the identification of emerging threat vectors unique to African networks, such as coordinated attacks on mobile payment platforms or irregular patterns in low-bandwidth financial systems.

Big Data analytics complements AI by providing the infrastructure to process vast, heterogeneous datasets derived from mobile networks, FinTech transactions, and telecom usage logs. In an African context, these data streams are critical for detecting trends in fraudulent activity, forecasting emerging threats, and enabling evidence-driven strategic decisions. For example, pattern analysis of mobile money agent transactions can reveal systemic vulnerabilities, while cross-referencing network logs with financial data can expose coordinated attacks across multiple platforms. The "Agentic Era" of AI in Africa necessitates the secure processing of autonomous systems' data, ensuring that the pipelines of information feeding AI models remain robust against manipulation or breaches (Chen et al., 2021; McKinsey, 2025). This approach moves the focus from static data storage to dynamic, real-time intelligence that is actionable and locally relevant.

Cloud Computing, as the third pillar, provides scalable, flexible, and cost-effective infrastructure that supports the deployment of AI and Big Data solutions across resource-constrained environments. African organizations, including SMEs and government institutions, often lack the capital to maintain extensive on-premises systems. Cloud-based environments enable the rapid implementation of sophisticated cybersecurity tools such as threat intelligence feeds, distributed denial-of-service (DDoS) mitigation, and encrypted storage solutions. However, a strictly imported cloud model can exacerbate risks related to data sovereignty and compliance with emerging regional regulations. An Afrocentric approach proposes localized or regional cloud infrastructures, coupled with Managed Shared Responsibility agreements, ensuring that cloud service providers take an active role in securing USSD and SMS-based financial transactions while African organizations retain oversight over critical data governance and operational policies (CIO Africa, 2025; Kearney, 2024).

The synthesis of literature highlights a critical knowledge gap: while AI, Big Data, and Cloud Computing are individually recognized as transformative tools, few studies explore their integrated

application within African socio-technical contexts. The proposed Afrocentric model addresses this gap by embedding principles of communal resilience and shared security drawing on the Ubuntu philosophy to foster collective threat intelligence. Crowdsourcing threat information through community networks aligns with African social structures more effectively than Western individualistic models, ensuring timely detection and mitigation of threats while respecting culturally informed privacy considerations.

These findings make a compelling case for an Afrocentric cybersecurity framework that is inherently tailored to the continent's vulnerabilities, infrastructures, and social realities. Rather than applying generic global solutions, such a model integrates AI, Big Data, and Cloud Computing in a manner that targets mobile-first threat vectors, empowers local expertise, strengthens data sovereignty, and supports digital self-determination. It moves cybersecurity beyond technical deployment into a contextually aware, culturally resonant, and strategically aligned discipline capable of sustaining Africa's digital future.

Conclusion

This study has systematically examined the evolving cybersecurity landscape in Africa, highlighting the inadequacy of prevailing Western-centric frameworks to address the continent's unique socio-cultural, economic, and infrastructural realities. The analysis demonstrates that while technologies such as Artificial Intelligence, Big Data, and Cloud Computing hold transformative potential, their application in Africa requires more than mere adoption; it demands an approach that is sensitive to local contexts, prioritizes data sovereignty, and incorporates indigenous knowledge systems.

The findings underscore that African cybersecurity challenges—ranging from the prevalence of mobile money fraud and USSD-based vulnerabilities to resource constraints and skill gaps—cannot be effectively mitigated by generic models that ignore communal practices, regulatory diversity, and culturally specific threat landscapes. The proposed Afrocentric model addresses this gap by integrating advanced technologies with principles grounded in African values and social structures, emphasizing community-based threat intelligence, capacity building, and localized cloud infrastructure.

By synthesizing the evidence, this study highlights that an Afrocentric approach moves beyond passive defense mechanisms, promoting proactive, culturally relevant, and sustainable cybersecurity strategies. Such an approach not only enhances technological resilience but also supports digital self-determination, ensuring that Africa can safeguard its citizens, institutions, and digital economies while actively shaping the architecture of its own cyberspace.

Finally, while the study provides a conceptual framework that integrates AI, Big Data, and Cloud Computing within an African-centered paradigm, it also identifies the need for future empirical validation. Testing the model in real-world contexts will be essential to refine its operationalization, assess its effectiveness, and ensure that it can adapt to the evolving cyber threat landscape while remaining responsive to local socio-cultural and economic conditions.

REFERENCES

360 Advanced. (2025, February 26). *The dark side of AI: New cybersecurity challenges for organizations*. https://360advanced.com/the-dark-side-of-ai-new-cybersecurity-challenges-for-organizations/

African Union. (2020). *African Union policy on cyber security*. Addis Ababa, Ethiopia: African Union Commission.

African Union. (2024). *Continental artificial intelligence strategy*. African Union Commission. https://au.int

African Union. (2025). *Cybersecurity in Africa: Annual report on threats, vulnerabilities, and responses*. AU Digital Economy & Cybersecurity Division. https://au.int/en

Akinyemi, O., Oladejo, O., & Adekunle, A. (2020). Artificial intelligence and cybersecurity in Africa: Prospects and challenges. *Journal of Information Security and Applications, 55*, 102615. https://doi.org/10.1016/j.jisa.2020.102615

Angin, P. (2019). Big data analytics for cyber security. *Published Special Issues*. https://doi.org/10.13140/RG.2.2.32403.66086

Anyoha, R. (2017). The history of artificial intelligence. *Science in the News, Harvard University*, 1–19.

Armbrust, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Asante, M. K. (1987). *The Afrocentric idea*. Temple University Press.

Chen, H., Chiang, R. H. L., & Storey, V. C. (2021). Business intelligence and analytics: From big data to big impact. *MIS Quarterly, 45*(1), 1–13.

CIO Africa. (2025, June 30). Who's driving AI-powered cybersecurity in Kenya and Africa? https://cioafrica.co/whos-driving-ai-powered-cybersecurity-in-kenya-and-africa/

CIO Africa. (2025a, April 3). How cloud migration strengthens IT security for African businesses. https://cioafrica.co/how-cloud-migration-strengthens-it-security-for-african-businesses/

CIO Africa. (2025b, March 6). The benefits of cloud computing for your business. https://cioafrica.co/the-benefits-of-cloud-computing-for-your-business/

Cisco Systems. (2024). *Cisco Annual Cybersecurity Report 2024*. Cisco. https://www.cisco.com/c/en/us/products/security/security-reports.html

Cobalt. (2025, December 23). Top cybersecurity statistics for 2025. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025

Cybersecurity Ventures. (2025). *Cybercrime report: Global damages reaching $10.5 trillion by 2025*. Cybersecurity Ventures.

De Villiers, I. (2024). The future of cyber security in Africa: Automating and predicting threats. *Cybersecurity Journal of Africa, 12*(3), 45–60.

Dumitras, T., & Shou, D. (2011). Toward a standard benchmark for computer security research: The Worldwide Intelligence Network Environment (WINE). In *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security* (pp. 89–96). Salzburg. https://doi.org/10.1145/1978672.1978683

Ekonde, D. (2025). *Africa and the AI race*. The Elephant. https://www.theelephant.info/ideas/2025/africa-and-the-ai-race

Ezekwueme Augustine, E., & Sunday, A. D. (2025). *Cybersecurity as a Pillar of Digital Sovereignty:* A Scoping Review in Rethinking Governance in Nigeria and West Africa.

Ezugwu, C. (2021). Artificial intelligence for cybersecurity in cloud computing: A review of recent advances. *IEEE Access, 9*, 323–337. https://doi.org/10.1109/ACCESS.2020.3049148

Hussain, F., & Alqahtani, S. (2021). Artificial intelligence for cybersecurity: Threats, challenges, and solutions. *Computers & Security, 104*, 102163. https://doi.org/10.1016/j.cose.2021.102163

IBM Security. (2025). *IBM X-Force Threat Intelligence Index 2025: Cybersecurity trends in emerging markets*. IBM. https://www.ibm.com/security/data

International Telecommunication Union. (2025). *Global cybersecurity index 2025: Africa regional report*. ITU. https://www.itu.int/en/ITU-D/Cybersecurity

Interpol. (2025, June 23). New INTERPOL report warns of sharp rise in cybercrime in Africa. https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

Kaopiz. (2025, April 8). *10 key benefits of cloud computing for businesses in 2025*. https://kaopiz.com/en/articles/10-key-benefits-of-cloud-computing-for-businesses-in-2025/

Kaur, R., et al. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kearney, A. (2024). *Cybersecurity challenges in Africa: Mobile Money and beyond*. Kearney Consulting.

Kinyua, G., & Kute, D. (2023). Empowering Africa: An in-depth exploration of the adoption of artificial intelligence across the continent. arXiv:2401.09457v1. https://arxiv.org/abs/2401.09457

KPMG International. (2023). *KPMG global cyber security outlook 2023: Navigating cyber risks in a complex environment*. KPMG. https://kpmg.com

Kumar, R., & Singh, S. (2020). Cyber threats to cloud computing: A comprehensive review. *Journal of Information Security and Applications, 55*, 102118.

Mbuyu, M. (2021). Digital transformation and cloud computing in Africa. *African Digital Economy Journal, 5*(2), 67–81.

McKinsey. (2025, May 15). AI is the greatest threat and defense in cybersecurity today. Here's why. https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today

MITRE. (2023). *Explainable AI in cybersecurity: Best practices and considerations.* MITRE Corporation. https://www.mitre.org/publications

Msukwa, L., & Dlodlo, N. (2021). Towards an Afrocentric cybersecurity framework for critical infrastructure in Southern Africa. *Journal of Cyber Security Technology, 5*(2), 89–105.

Organisation for Economic Co-operation and Development. (2023). *Enhancing the digital security of SMEs*. OECD Publishing. https://www.oecd.org

Palo Alto Networks. (2025). *Unit 42 Threat Report 2025*. Palo Alto Networks. https://www.paloaltonetworks.com/resources

Rao, A. S., & Verweij, G. (2017). *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* PwC. https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020). Machine learning and deep learning techniques for cybersecurity: A review. In *Advances in Intelligent Systems and Computing* (pp. 50–57). Springer. https://doi.org/10.1007/978-3-030-44289-7_5

StationX. (2025, April 25). 10 examples of AI in cyber security (latest research). https://www.stationx.net/examples-of-ai-in-cyber-security/

Tremhost, J. (2025). Mobile money fraud trends and mitigation in sub-Saharan Africa. *FinTech Security Review, 12*(1), 33–50.

World Bank. (2022). *Digital development in Africa: Infrastructure and cloud adoption trends*. World Bank Group. https://www.worldbank.org

World Economic Forum. (2025). *Global risks report 2025: Technology and cybersecurity*. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592