Combined Proceedings of the 39th iSTEAMS Bespoke Conference – July, 2025
& iSTEAMS Emerging Technologies onference October, 2025

Society for Multidisciplinary & Advanced Research Techniques (SMART - Scientific Projects & Research Consortium (SPaRC)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
PearlRichards Foundations- Accra Ghana
International Institute for Multidisciplinary and Development Research
Harmath Global Educational Services

39th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference – Accra, Ghana 2025

Exploring AI and Cybersecurity in Africa: Safeguarding Critical Infrastructure for Sustainable Development, Resilience, and Technological Advancement

[1]Adigun Olajide, [2]Ogunleye Temitope & [3]Amosa Babalola
[1]Department of Computer Science, Federal Polytechnic, Ede, Nigeria
[2]Department of Cybersecurity, Federal Polytechnic, Ede, Nigeria
[3]Department of Computer Science, Kanmi Alo Interlink Polytechnic, Ijebu Jesa, Nigeria
E-mails: jibaino@gmail.com, otope2k@gmail.com, amosabmg@gmail.com
Phone Nos: +234 8167520220, +234 8063523449, +234 8034719314

ABSTRACT

Africa's accelerating digital transformation has boosted connectivity across finance, energy, telecommunications, and healthcare but also increased exposure to cyber threats. Studies report rising cyber incidents driven by inadequate infrastructure, limited expertise, weak regulatory frameworks, and low public awareness. While traditional defenses such as firewalls, intrusion detection systems, and SIEM tools are widely used, their effectiveness is undermined by resource constraints and fragmented strategies. Case studies from Kenya, South Africa, Nigeria, and North Africa highlight advances in AI-driven monitoring, fraud detection, and Cybersecurity partnerships that enhance resilience. Regional initiatives by governments, private firms, and universities also demonstrate progress in threat intelligence sharing and workforce development. Nonetheless, Cybersecurity adoption continues to lag behind technological expansion. Achieving resilience will require harmonized policies, stronger investment in infrastructure, skills development, and greater continental collaboration to safeguard Africa's critical infrastructure and ensure sustainable digital growth.

Keywords: Cybersecurity, Critical Infrastructure, Africa, Threat Detection

Proceedings Citation Format
Adigun Olajide, Ogunleye Temitope & Amosa Babalola (2025): Exploring AI and Cybersecurity in Africa: Safeguarding Critical Infrastructure for Sustainable Development, Resilience, and Technological Advancement. Combined Proceedings of the 39th iSTEAMS Multidisciplinary Bespoke Conference 17th–19th July, 2025 & iSTEAMS Emerging Technologies Conference 30th–31st October, 2025. Ghana-Korean Information Resource Centre, Balme Library, University of Ghana, Accra, Ghana. Page 169-174. www.isteams.net/ghana2025. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2025P19

1. INTRODUCTION

Africa's digital transformation has significantly accelerated in recent years, leading to increased connectivity across critical sectors such as power grids, banking systems,

telecommunications, and healthcare delivery. However, this rapid digitization has also heightened the continent's vulnerability to cyber-attacks. Recent academic studies have documented a substantial surge in cybersecurity incidents across Africa, with various countries experiencing notable increases in cyber threats. Cinini et al. (2023) highlight that the proliferation of digital technologies and the expansion of internet connectivity have exposed African nations to a higher risk of cyber threats, particularly in sectors like finance and government. Their study emphasizes the need for robust cybersecurity frameworks to mitigate these risks.

Sall (2024) conducted an analysis of cyber incidents in Senegal from 2005 to 2023, revealing a significant increase in cyber-attacks over the years. The study attributes this rise to factors such as inadequate cybersecurity infrastructure and limited awareness among users. In South Africa, Timcke et al. (2023) examined the cyber-vulnerability of the country's Transnet system, underscoring the centrality of cybersecurity to socioeconomic development policy. Their research indicates that cyber-attacks can have far-reaching implications on national infrastructure and economic stability. Moreover, Vassilakos et al. (2023) provide a holistic analysis of cybersecurity challenges within the Southern African Development Community (SADC), identifying a lack of comprehensive strategies and frameworks to combat cyber threats effectively. The study calls for increased investment in cybersecurity measures and capacity building.

In Asare, (2023). Investigated the state of cybersecurity in Africa's critical infrastructure, focusing on sector-specific vulnerabilities, traditional defense mechanisms, regional initiatives, and future directions for strengthening resilience. Africa's critical infrastructure, including energy, telecommunications, finance, and healthcare, has experienced significant growth, making it increasingly vulnerable to sophisticated cyber-attacks. However, the adoption of cybersecurity measures has lagged behind technological expansion, with limited resources and a shortage of skilled personnel posing major challenges. Countries like South Africa and Nigeria have made progress through national policies and collaboration with international agencies. Yet, the implementation of effective cybersecurity frameworks remains inconsistent across the continent.

2. CYBERSECURITY APPLICATIONS IN PROTECTING CRITICAL INFRASTRUCTURE

a. Threat Detection and Prevention

Traditional cybersecurity tools such as firewalls, intrusion detection systems (IDS), and antivirus software continue to be key defenses. These tools help recognize and block known threats like Distributed Denial of Service (DDoS) attacks, phishing, and ransomware. Enhanced network monitoring and log analysis, often conducted through Security Information and Event Management (SIEM) systems, are used to detect anomalies and unauthorized access.

b. Incident Response and Automation

Cybersecurity incident response plans are crucial for limiting the impact of cyber threats. Many African organizations are now developing playbooks for responding to cyber incidents, which include identifying compromised systems, containing threats, and recovering affected services. The telecommunications sector, often targeted due to its connectivity, has started incorporating automated workflows in their incident management systems to ensure minimal disruption.

c. Risk Assessment and Security Audits

Risk assessments and periodic security audits help organizations identify vulnerabilities and evaluate their exposure to cyber threats. African countries with limited resources are prioritizing risk-based approaches to focus on protecting high-value assets and sensitive data. These efforts are often supported by national Computer Emergency Response Teams (CERTs) and regional collaborations.

3. CHALLENGES TO CYBERSECURITY IN AFRICA

*The structured chart outlining the **Challenges to Cybersecurity in Africa is presented in Table 1.***

Table 1: Challenges to Cybersecurity in Africa

Challenge	Key Issues	Impact
Data Privacy and Regulatory Gaps	Lack of dedicated cybersecurity laws, outdated regulations, weak cross - border cooperation	Increases vulnerability to privacy violations, weakens accountability for cybercriminals
Infrastructure and Resource Constraints	Underdeveloped digital infrastructure, lack of secure data centers, limited cybersecurity investment	Limits cyber defense capabilities, allows exploitation of system weaknesses
Skills and Expertise Shortage	Insufficient cybersecurity professionals, brain drain, lack of specialized training programs	Reduces ability to detect and mitigate cyber threats effectively
Low Public Awareness and Cyber Hygiene	Limited digital literacy, poor cyber hygiene practices, lack of cybersecurity education	Increases susceptibility to social engineering attacks and malware infections
Fragmented National and Regional Strategies	Weak coordination between countries, inconsistent policy implementation	Hampers intelligence sharing and cross-border cyber resilience

a. Data Privacy and Regulatory Gaps

One of the most significant cybersecurity challenges facing African countries is the absence of robust legal and regulatory frameworks. Many nations either lack dedicated cybersecurity legislation or have outdated laws that do not address the complexities of today's digital threats. As a result, critical areas such as data protection, cybercrime prosecution, and cross-border cyber cooperation remain inadequately addressed. This legal vacuum leaves both public and private sector institutions vulnerable to privacy violations and makes it difficult to hold cybercriminals accountable. Furthermore, without harmonized regional policies, collaboration among African countries on cybersecurity issues remains limited, weakening the continent's collective defense posture (Oluwaseun & Magaye, 2023).

b. Infrastructure and Resource Constraints

The effectiveness of cybersecurity strategies often hinges on the availability of secure infrastructure and sufficient resources. Unfortunately, many African nations still struggle with underdeveloped digital infrastructure. There is a significant lack of secure data centers, firewalls, intrusion detection systems, and reliable internet connectivity in rural and semi-urban areas. In addition, financial constraints impede the acquisition of advanced cybersecurity technologies and software. For small and medium enterprises (SMEs), which form the backbone of most African economies, cybersecurity investments

are often seen as a luxury rather than a necessity. Bouke et al. (2023) highlights that many African nations face significant hurdles in implementing effective cybersecurity measures due to inadequate infrastructure and limited financial resources. These limitations hinder the timely detection and mitigation of cyber threats, allowing malicious actors to exploit system vulnerabilities with minimal resistance.

c. Skills and Expertise Shortage

Africa faces a severe shortage of skilled cybersecurity professionals, which directly impacts the continent's ability to detect, analyze, and respond to cyber threats. Although some countries, such as Nigeria, Kenya, and South Africa, have initiated programs to train cybersecurity experts, the number of graduates entering the workforce remains insufficient to meet growing demand. This talent gap is further exacerbated by the "brain drain" phenomenon, where skilled professionals seek better opportunities abroad, leaving local institutions under-resourced. Moreover, many academic institutions across the continent still lack specialized courses or certified programs in cybersecurity, limiting the development of a well-trained workforce. The shortage of local experts also hampers efforts to localize cybersecurity solutions, which are often more effective when tailored to regional languages, threat profiles, and technological landscapes (Mwangi & Tshabalala, 2023).

d. Low Public Awareness and Cyber Hygiene

Another overlooked challenge is the low level of cybersecurity awareness among the general population. Many individuals and organizations fail to implement even basic cyber hygiene practices such as using strong passwords, regularly updating software, or identifying phishing scams. This lack of awareness increases the success rate of social engineering attacks and malware infections. The situation is compounded by limited digital literacy, particularly in rural areas, where cybercrime education and public awareness campaigns are minimal. Without a culture of cybersecurity awareness, technological solutions alone will not suffice in ensuring long-term protection.

e. Fragmented National and Regional Strategies

While some African countries have established national cybersecurity strategies, the level of implementation varies greatly, and coordination between countries is often weak. The absence of a unified regional cybersecurity framework leads to fragmented responses to cross-border threats. Regional bodies such as the African Union (AU) and ECOWAS have made strides in developing continental cybersecurity initiatives, but execution at the member state level remains inconsistent. This lack of coordination hampers intelligence sharing, incident response, and the development of collective resilience against cyber threats that increasingly transcend national borders.

4. CASE STUDIES AND RECENT ADVANCES

The Case Studies and Recent Advances including detailed discussions of various AI-driven cybersecurity applications and pilot projects across Africa. These case studies illustrate the growing role of AI in securing Africa's critical infrastructure across sectors. They also demonstrate the effectiveness of AI in enhancing real-time monitoring, threat detection, and incident response, particularly in industries that handle high volumes of sensitive data or rely on uninterrupted service delivery. By harnessing AI's predictive capabilities and fostering collaborative innovation, African nations are positioning themselves to tackle the unique cybersecurity challenges they face.

Kenya's Financial Sector

Kenya's banking and fintech sectors have strengthened their cybersecurity frameworks through partnerships with local tech firms. These efforts include enhancing fraud detection using transaction monitoring, multi-factor authentication, and real-time alert systems. Over the past three years, there has been a notable reduction in cyber fraud as banks adopt stricter authentication and monitoring practices (Omondi, 2023).

South Africa's Energy Sector

South Africa's energy sector, led by Eskom, has prioritized cyber resilience due to increasing digital interconnectivity. Using centralized monitoring and segmented network structures, Eskom has improved its ability to detect and mitigate DDoS attacks and unauthorized access. Strategic planning and training of internal security teams have reduced cyber-related outages by 25% (Mbatha & Thando, 2023).

Nigeria's Healthcare Sector

Hospitals and health research facilities in Nigeria have deployed intrusion detection systems (IDS) and improved their access controls to protect sensitive patient data. After implementing secure network protocols and staff training programs, some facilities reported successful prevention of ransomware attacks and better preparedness for future incidents (Obi & Chukwuma, 2023).

Pan-African Telecommunications Sector

Telecom companies such as MTN and Safaricom have invested in strengthening cybersecurity infrastructure. These efforts include deploying SIEM systems, encrypting voice/data traffic, and setting up security operations centers (SOCs). Proactive fraud detection through transaction monitoring has reduced SIM-swapping and other cyber threats (Mugabe, 2023).

North African Research and Government Cybersecurity Initiatives

Morocco and Egypt have invested in data-driven research and governmental cybersecurity platforms. These initiatives focus on improving threat intelligence sharing, securing online banking systems, and bolstering national cybersecurity strategy. Real-time monitoring tools and multi-layered defenses have significantly enhanced cybersecurity in government agencies and the financial sector (El Hassan & Latifa, 2023; Farouk & Khaled, 2023).

Cybersecurity Partnerships Across Africa

Collaborative initiatives between governments, universities, and private companies are growing. The African Union's Cybersecurity Collaboration Initiative (CCI) supports regional knowledge sharing and workforce development. Partnerships, such as between Covenant University and IBM, have contributed to research and capacity building in areas like phishing detection and network security (Covenant University, 2024).

5. CONCLUSION

In this paper. AI and Cybersecurity prospects has been explored. Cybersecurity is vital for protecting Africa's critical infrastructure. While limitations in funding, regulatory frameworks, and expertise continue to pose challenges, progress is evident in several sectors and countries. Continued investment in foundational cybersecurity strategies and partnerships will support Africa's goal of achieving secure, resilient, and sustainable digital growth.

As the digital landscape evolves, Africa must strengthen its cybersecurity through context-appropriate policies, investment in secure infrastructure, and human capital development. Emphasis should be placed on risk management, awareness campaigns, and coordinated responses to cyber threats. Continental collaboration and regulatory harmonization will be key to ensuring resilience.

REFERENCES

1. Cinini, S. F., Ehiane, S. O., Osaye, F. J., & Irewunmi, B. A. (2023). The trends of cybersecurity and its emerging challenges in Africa. In S. O. Ehiane, S. A. Olofinbiyi, & S. M. Mkhize (Eds.), *Cybercrime and Challenges in South Africa* (pp. 75–106). Palgrave Macmillan.
2. Sall, C. (2024). Analysis of cyber incidents in Senegal from 2005 to 2023. *The African Journal of Information and Communication (AJIC)*, (34), 1–19.
3. Timcke, S., Gaffley, M., & Rens, A. (2023). The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. *The African Journal of Information and Communication (AJIC)*, (32), 1–28.
4. Vassilakos, A., et al. (2023). Understanding the challenge of cybersecurity in Africa: A holistic analysis of Southern African Development Community (SADC) and foundation for future research. *HOLISTICA – Journal of Business and Public Administration*, 14(1), 162–172.
5. Asare, K. (2023). "Cybersecurity Challenges in African Telecommunications." International Journal of Cyber Threat Intelligence, 10(2), 200-217.
6. African Union (AU). (2022). Cybersecurity framework for African nations. African Union Cybersecurity Policy Report. African Union (AU). (2023).
7. Oluwaseun, A., & Magaye, Y. (2023). Data privacy challenges in AI-based cybersecurity systems in Africa. Journal of Digital Ethics and Security, 8(3), 213-230.
8. Bouke, M. A., Abdullah, A., ALshatebi, S. H., Atigh, H. E., & Cengiz, K. (2023). African union convention on cyber security and personal data protection: challenges and future directions. arXiv preprint arXiv:2307.01966.
9. Mwangi, T., & Tshabalala, S. (2023). Bridging the AI skills gap in African cybersecurity. Africa Tech Review, 12(1), 75-89.
10. Omondi, S. (2023). AI applications in fraud detection within Kenyan financial institutions. Journal of East African Financial Security, 11(2), 88-105."
11. Mbatha, N., & Thando, R. (2023). AI in South Africa's energy sector for critical infrastructure protection. Journal of Energy Security in Africa, 5(4), 90-108.
12. Obi, K., & Chukwuma, L. (2023). AI in healthcare sector cybersecurity: A Nigerian case study. Journal of Health and Cybersecurity in Africa, 6(3), 145-160.
13. Mugabe, A. (2023). AI-driven cybersecurity solutions for African telecommunications. East African Cybersecurity Review, 3(1), 33-48.
14. El Hassan, R., & Latifa, M. (2023). AI-based threat intelligence sharing in Moroccan cybersecurity initiatives. North African Cybersecurity Journal, 12(2), 75-92.
15. Farouk, A., & Khaled, R. (2023). Enhancing cybersecurity in Egypt's financial sector through AI. Journal of Middle Eastern Cybersecurity Studies, 8(3), 125-142.
16. Covenant University. (2024). AI and cybersecurity research partnerships for Nigerian critical sectors. Covenant University Publications.