International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 47 No. 2 November 2024, pp. 459-468

Reimagining Urban Security: Ai Solutions To Cyber Threats In African Smart Cities, Drawing Insights From The Eu

Anya Adebayo, ANYA [1], kelechi Adura, ANYA [2], Eke Kehinde ANYA [3], Akinwale Victor, ISHOLA [4]

[1]Department of Political Science, Obafemi Awolowo University Ile-Ife
adeanya@summalogix.com
[2]Computer science, Landmark University Omu-Aran Nigeria
anyakelechiadura@gmail.com
[3]Scottish Power Headquarters, Glasgow
eanya@spenergynetworks.co.uk
[4]Department of Peace, Security and Humanitarian Studies, University of Ibadan
victorakinwale2@gmail.com

Abstract – This paper critically examines the intersection of cybersecurity and artificial intelligence (AI) within the advancing framework of smart city development in Africa. As urban centres across the continent adopt Internet of Things (IoT)-enabled systems to enhance efficiency and public service delivery, they encounter complex cybersecurity challenges, such as data breaches, malware attacks, and infrastructure vulnerabilities. Utilizing insights from established European Union (EU) cybersecurity frameworks, this study investigates both the current landscape of cyber threats in African smart cities and the transformative potential of AI-driven solutions to enhance urban security.

The paper reiterates AI's role in bolstering urban cybersecurity through automated threat detection, real-time incident response, and predictive analytics. To facilitate implementation, the study identifies key strategies such as fostering local expertise, promoting public-private partnerships, and supporting innovation hubs focused on AI research for urban security applications. Policy adaptations are also recommended, including the establishment of open data standards, data localization measures, and inclusive governance frameworks, to support the sustainable integration of AI in urban security. In alignment with EU policy frameworks on data protection and system interoperability, these recommendations aim to empower African policymakers and urban planners with actionable approaches to effectively mitigate cyber risks in smart city contexts.

This paper argues that African smart cities, by embracing tailored AI-driven cybersecurity solutions alongside adaptive policy frameworks, can achieve secure, resilient urban systems that capitalize on digital transformation while safeguarding public data and critical infrastructure.

Keywords – Urban security, Cyber security, Cyber threats, Smart cities.

INTRODUCTION

The rapid growth of smart cities worldwide represents a transformative shift in urban development, leveraging digital technology to optimize public services, infrastructure, and resource management (Gracias et al, 2023). Across Africa, several cities are embracing this trend, aiming to address urban challenges such as population growth, resource management, and economic development. However, as cities in Africa integrate IoT devices, data networks, and cloud-based solutions, they also become increasingly vulnerable to cyber threats. With critical systems like transportation, healthcare, and utilities reliant on digital networks, the consequences of cyber-attacks could be severe, threatening not only infrastructure but also public safety and privacy.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 47 No. 2 November 2024, pp. 459-468

In response to these rising cybersecurity challenges, artificial intelligence (AI) has emerged as an essential tool for urban security in smart cities. AI-driven cybersecurity solutions offer capabilities such as real-time threat detection, predictive analytics, and automated responses that are crucial for protecting the complex, interconnected systems of a smart city. By continuously monitoring network activity, AI can detect anomalies and respond swiftly, preventing potential breaches before they escalate. Additionally, AI can analyze vast amounts of data far beyond human capability, which is essential for managing the high data volume generated by smart city infrastructures.

Africa's journey toward secure smart cities can benefit significantly by drawing insights from the European Union (EU), a region with extensive experience in both smart city development and robust cybersecurity frameworks. The EU has pioneered policies, like the General Data Protection Regulation (GDPR), which address privacy and data security, and supports initiatives that advance AI-based cybersecurity solutions. These frameworks and practices are valuable to African smart city projects, which can adopt or adapt these insights to address the unique challenges they face.

Statement of the problem

As African cities increasingly adopt smart city initiatives, integrating advanced technologies to improve urban life, they face a critical vulnerability: cybersecurity. The interconnected infrastructure of a smart city, spanning utilities, healthcare, transportation, and public safety, relies heavily on digital networks and data exchange, making it a prime target for cyber threats. These threats, ranging from data breaches and ransomware to system hijacking, have far-reaching implications for public safety, privacy, and economic stability. Despite the rapid digital transformation underway in many African urban centres, existing cybersecurity frameworks and resources remain inadequate to effectively counter these risks.

Artificial intelligence (AI) has emerged as a promising solution to enhance cybersecurity, offering tools for real-time threat detection, predictive analysis, and rapid response capabilities essential for safeguarding smart city infrastructures. However, the adoption of AI-driven cybersecurity solutions in Africa is limited by factors such as resource constraints, regulatory gaps, and the need for technical expertise. Additionally, while African cities face unique challenges, they can gain valuable insights from established practices and regulatory frameworks, such as those implemented by the European Union (EU), which has achieved significant advancements in cybersecurity and AI application within its smart cities.

This paper addresses the pressing need for robust AI-powered cybersecurity solutions tailored to African smart cities, drawing lessons from EU experiences. Given the critical importance of securing digital infrastructures for sustainable urban growth, it is on this backdrop that this paper seeks to examine actionable AI-driven strategies that can be adapted from the EU context to effectively mitigate cyber risks within African cities. By exploring these insights, this paper aims to contribute to the development of resilient cybersecurity frameworks that support the secure and sustainable evolution of African smart cities.

Cybersecurity Challenges in African Smart Cities

The development of smart cities in Africa, as with other parts of the world, is rapidly advancing, leveraging innovative technologies to improve urban life. However, as Ahmad et al. (2024) note, this transformation introduces significant cybersecurity challenges, largely due to the extensive interconnection of digital systems. In a smart city environment, the convergence of networks, services, and devices, ranging from public utilities and transportation systems to emergency response networks, creates an expansive digital ecosystem that is increasingly vulnerable to cyberattacks. This interconnectedness is a double-edged sword: while it enables more efficient and responsive urban services, it also provides potential attackers with an extensive "attack surface" that can be exploited for various forms of cyber threats, including data breaches, system hacking, and malware attacks (Oliha et al., 2024).

One key vulnerability in African smart cities, highlighted by Oliha et al. (2024), lies in the proliferation of Internet of Things (IoT) devices that often lack adequate security measures. These devices, ranging from sensors and cameras to smart utilities and traffic management systems, are frequently designed with limited attention to cybersecurity, rendering them susceptible to exploitation. As these devices form the backbone of many smart city functions, their compromise can lead to cascading effects across various sectors. For instance, a breach in IoT networks could disrupt essential services, impact public safety, and expose sensitive personal and governmental data.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 47 No. 2 November 2024, pp. 459-468

Africa's cybersecurity landscape is further complicated by a combination of rapid ICT growth and insufficient regulatory frameworks. Adomako et al. (2018) underscore the fact that, while ICT adoption is accelerating across the continent, legislative responses have not kept pace. Only 11 out of 54 African nations have enacted specific cybercrime laws, meaning that the majority lack effective legal provisions to address the evolving nature of cyber threats. This regulatory gap leaves African cities exposed, as the absence of robust legal frameworks inhibits the implementation of preventive cybersecurity measures, enforcement actions, and effective response strategies. Furthermore, this lack of legislation limits the ability of African nations to cooperate in cross-border cybersecurity initiatives, which is crucial given the global and interconnected nature of cyber threats.

In addition to regulatory challenges, Africa also suffers from a pronounced shortage of cybersecurity professionals. According to Adomako et al. (2018), the continent has only one certified security professional for every 177,000 people, indicating a substantial skills gap that weakens the capacity of African smart cities to defend against and respond to cyber incidents. The limited availability of trained cybersecurity personnel not only slows down the development of secure systems but also constrains the ability of cities to monitor, identify, and mitigate potential threats effectively. This skills deficit underscores an urgent need for investment in cybersecurity training and capacity building to equip Africa's workforce with the necessary skills to manage and secure smart city infrastructures.

The policy landscape in Africa also reveals a tension between maintaining internet freedoms and implementing effective cybersecurity controls. Turianskyi (2018) notes that African governments face the complex challenge of balancing these priorities, particularly as the proliferation of digital services has brought both social and economic benefits to urban populations. Efforts to strengthen cybersecurity policies could, however, risk curtailing digital rights if not carefully managed, posing an additional hurdle to the formulation of cohesive and effective cybersecurity regulations.

The Draft African Union Convention on Cybersecurity, though intended to establish a framework for cybersecurity governance across the continent, has faced criticism for its shortcomings in effectively promoting cybersecurity and controlling cybercrime. Orji (2012) argues that the convention fails to address core issues in cyber governance and lacks clear mechanisms for enforcement and compliance. This criticism reflects broader challenges in formulating regionally coherent cybersecurity policies that can address the diverse and rapidly evolving threats facing smart cities across African nations. The convention's limitations suggest that a more robust and enforceable regional framework may be necessary to unify and strengthen Africa's cybersecurity posture.

Comparative Observations on EU Cybersecurity Challenges

While cybersecurity challenges in Africa are unique, it is instructive to also examine parallels with other regions. For instance, the EU also faces challenges in coordinating cybersecurity efforts across member states and addressing the technical and regulatory complexities of securing smart city infrastructures. Ilves et al. (2016) point out that the EU and NATO have increasingly recognized cyber threats as integral components of modern security conflicts, acknowledging that future hostilities are likely to involve both cyber and physical elements. The EU's efforts to build collaborative cybersecurity strategies demonstrate the complexities involved in achieving cohesive cybersecurity governance within a multi-state framework.

The structure of EU cybersecurity governance, however, has faced hurdles, particularly in the public procurement process for cybersecurity services. Ruohonen (2019) highlights that public cybersecurity procurement in the EU encounters competition barriers and has not yet reached a level of "Europeanization" that allows for consistent, continent-wide approaches. This gap underscores a significant challenge in creating unified cybersecurity responses across member states, suggesting that even well-resourced regions like the EU grapple with regulatory fragmentation and alignment issues. These challenges may resonate with Africa's need for more coordinated cybersecurity strategies and frameworks.

Another dimension of the EU's cybersecurity landscape is its value-driven approach, where regulatory policies aim to uphold fundamental rights such as privacy and data protection. Jasmontaite et al. (2017) observe that the EU's commitment to these values occasionally generates friction between security measures and the protection of individual rights, reflecting the ongoing debate about the appropriate balance between security and civil liberties. This tension is echoed in Africa's cybersecurity discourse, where governments grapple with the dual objectives of enhancing security and maintaining internet freedoms (Turianskyi, 2018).

Recent regulatory advancements, such as the EU Cybersecurity Act of 2019, highlight efforts to centralize cybersecurity governance by empowering agencies like the European Union Agency for Cybersecurity (ENISA) with broader mandates (Romaniuk et al., 2020). This regulatory model underscores the potential benefits of streamlined governance structures, suggesting that centralized cybersecurity institutions can enhance the effectiveness of policy enforcement and improve coordination in cyber incident response. For African smart cities, such models may be instructive in the long term, though they would require adaptations to account for local needs and governance constraints.

AI-Driven Cybersecurity Solutions

Artificial Intelligence (AI) is increasingly recognized as a critical component in cybersecurity, particularly as the complexity and frequency of cyber threats escalate. AI's capacity for data-driven decision-making, facilitated by machine learning algorithms, enables real-time analysis of vast datasets to detect patterns and anomalies that suggest potential cyber threats (Rizvi, 2023; Camacho, 2024). These capabilities mark a significant shift from traditional, largely reactive cybersecurity measures, allowing for proactive threat detection and swift intervention. In smart cities, where interconnectivity and data exchange occur at an unprecedented scale, AI's ability to autonomously identify and mitigate risks is indispensable to ensuring operational continuity and urban security.

AI's contribution to cybersecurity extends beyond detection to include automated incident response systems. These systems leverage machine learning to autonomously assess risk, analyse data, and initiate containment strategies in response to threats, thereby reducing reliance on manual oversight and minimizing response times (Rizvi, 2023). For smart cities, where interruptions in critical infrastructure systems, such as transportation, healthcare, or utilities, can have immediate and profound impacts, the capacity for rapid, AI-driven incident response is essential. This shift from reactive defence to dynamic, automated response frameworks represents a significant enhancement in the ability of smart city security protocols to protect against disruptions caused by cyber incidents.

Furthermore, AI applications in cybersecurity include specialized deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), which are employed for tasks like malware classification, intrusion detection, and threat intelligence (Li, 2018; Chen et al., 2020). CNNs, for instance, are adept at identifying complex patterns within malware datasets, while RNNs are particularly effective in analyzing sequential data for signs of network intrusion. These models surpass traditional systems in their ability to recognize and categorize sophisticated cyber threats, providing a tailored approach to combating the diverse range of threats encountered in the dynamic environments of smart cities.

Additionally, AI-driven cybersecurity strategies incorporate advanced technologies such as natural language processing (NLP) and knowledge-based expert systems, which enhance the automation and efficacy of cybersecurity processes (Sarker et al., 2021). NLP enables the analysis of unstructured data, such as security logs and threat reports, offering valuable insights into emerging threat landscapes and facilitating pre-emptive responses. Knowledge-based systems, designed to simulate human expertise, further augment AI's role in decision-making by offering intelligent recommendations and guidance, particularly in complex or novel threat scenarios. By automating these high-level functions, AI not only addresses the limitations of human capacity in managing cybersecurity demands but also establishes a more resilient defence architecture within the smart city context.

Without a doubt, AI's role in cybersecurity for smart cities is transformative, providing enhanced capabilities for detection, analysis, and response that traditional systems cannot achieve. As smart cities continue to evolve, AI-driven cybersecurity frameworks will likely remain central to safeguarding urban infrastructure, ensuring that smart cities can maintain their functionality and safety in the face of increasingly sophisticated cyber threats. This reliance on AI underscores the necessity of ongoing advancements in machine learning and deep learning technologies to sustain and enhance urban security in an era of rapid digital integration.

Challenges in implementing AI

The integration of AI-driven cybersecurity solutions in African smart cities faces significant challenges, many of which stem from both infrastructural limitations and contextual concerns specific to the region. Resource constraints represent a primary obstacle, with many African cities lacking the substantial financial investments necessary to develop and deploy sophisticated AI technologies

(Nibigira et al., 2024). This limited financial capacity also hampers local research and development efforts, restricting the advancement of homegrown AI solutions tailored to the unique cybersecurity needs of African smart cities. Without sufficient funding, these cities are often reliant on foreign technologies that may not fully address or align with the local context.

Another pressing challenge is the shortage of skilled talent in AI and cybersecurity domains across the continent. Africa's labour market exhibits a marked gap in technical expertise, with a limited pool of professionals trained in AI, machine learning, and cybersecurity (Nibigira et al., 2024). This talent deficit complicates efforts to build and maintain resilient AI-driven security systems, making it difficult for cities to implement and optimize these technologies effectively. Consequently, the dependence on external expertise can delay response times to threats and reduce the efficacy of AI implementations in rapidly evolving smart city environments.

Ethical and social considerations also play a significant role in the challenges of AI deployment. AI systems in cybersecurity often make critical, real-time decisions that impact citizens' safety and privacy, raising concerns about accountability and transparency (Nibigira et al., 2024). Furthermore, the design and application of AI must consider issues such as gender equity and cultural diversity to prevent biases that may disproportionately affect certain groups (Gwagwa et al., 2020). Failure to address these ethical dimensions can exacerbate existing social inequalities and reduce public trust in AI applications, potentially hindering the adoption of these technologies in urban security frameworks.

The complex, interconnected nature of smart city infrastructure itself presents an additional layer of vulnerability. As more services and systems become digitally integrated, the "attack surface" expands, exposing critical infrastructure, including energy grids, transportation systems, and communication networks, to an array of cyber threats (Ahmad et al., 2024). This interconnectivity means that a breach in one area could have cascading effects across multiple sectors, amplifying the potential impact of a cyberattack. AI-driven attacks add further complexity, as malicious actors can harness machine learning techniques to bypass traditional security measures, thereby necessitating highly adaptive and advanced defence mechanisms that many African cities are currently unable to implement (Familoni, 2024).

Insights from EU Cybersecurity Frameworks

Overview of EU Cybersecurity Policies

The European Union (EU) has established a comprehensive set of policies and regulations to address cybersecurity challenges, particularly within smart city contexts. A cornerstone of these initiatives is the General Data Protection Regulation (GDPR), which provides a unified framework for data protection across EU member states. GDPR directly impacts the way smart cities operate, as it mandates strict guidelines on how personal data is collected, processed, and stored, reinforcing data privacy and security within urban digital infrastructures (Stefanouli & Economou, 2018). One essential GDPR requirement for smart cities is the Data Protection Impact Assessment (DPIA), a process that evaluates potential privacy risks associated with new data-intensive services. Conducting DPIAs can be resource-intensive, with costs that vary based on the specific urban environment and the nature of the services provided. This adds financial and operational complexity for city administrators aiming to implement GDPR-compliant technologies in diverse urban settings (Vandercruysse et al., 2020).

In addition to GDPR, the EU has implemented sector-specific guidelines under the Network and Information Security (NIS) Directive, which emphasizes a cross-sectoral approach to cybersecurity, making it applicable to critical infrastructure within smart cities. This directive provides both general cybersecurity principles and sector-specific recommendations, fostering resilience across industries, from healthcare to transportation, that form the backbone of smart city ecosystems (Škundrić et al., 2022). By aligning with international cybersecurity standards, the EU's initiatives support a broader framework for urban safety and digital inclusivity, furthering the objectives of the United Nations Sustainable Development Goal 11, which advocates for safe and sustainable urban development through ICT advancements.

However, ethical concerns about the management and use of sensitive data in smart city settings continue to challenge policymakers and urban planners. While GDPR provides a robust legal framework for data protection, balancing the benefits of data-driven services with ethical responsibilities remains complex. This legal model has been noted for its potential to guide other regions

aiming to protect citizens' rights within increasingly digitized urban environments, yet it also highlights the need for continuous refinement as technologies evolve (El Khafif & Salem, 2021). The EU's experience underscores the importance of adaptable, ethical governance structures in cybersecurity, which are essential for achieving secure, inclusive, and technologically advanced cities.

Successful AI Use Cases in EU Smart Cities

European smart cities have seen considerable success in implementing AI and IoT solutions to improve urban efficiency, sustainability, and quality of life. In Amsterdam, AI-driven systems analyze citizen complaints, facilitating faster response times and more effective public service management (Mark & Anya, 2019). Similarly, Helsinki has adopted a parking permit chatbot that uses AI to simplify parking management for residents, making it easier for citizens to access municipal services and reducing administrative burdens. Cities like Copenhagen and Hamburg have invested in advanced data exchange platforms, which enable seamless data sharing across various urban sectors, enhancing service delivery and fostering interdepartmental collaboration (Mark & Anya, 2019).

In Aveiro, Portugal, the integration of AI with IoT in urban infrastructure has led to substantial gains in traffic management, energy optimization, and safety. The city's intelligent management system monitors and adjusts traffic flow, reducing congestion and improving public safety. By employing AI to monitor energy consumption, Aveiro also contributes to sustainability goals by minimizing waste and promoting efficient resource use. Additionally, the system detects and addresses infrastructure issues, providing pre-emptive maintenance alerts that reduce disruptions and improve the resilience of critical city services (Dias et al., 2023).

The SUPERHUB Project further illustrates AI's capacity to enhance smart city capabilities. This initiative, which focuses on smart mobility, integrates AI to optimize transportation options, increase urban competitiveness, and encourage citizen engagement in decision-making processes. By aligning ICT solutions with user-friendly applications, SUPERHUB fosters a more dynamic and connected urban environment, underscoring AI's role in facilitating sustainable urban mobility (Vázquez-Salceda, 2014; Salceda et al., 2014).

These European case studies highlight the transformative potential of AI in urban governance, illustrating how AI-driven solutions can make cities more adaptive, efficient, and responsive to the evolving needs of their residents. As African cities continue to explore smart city initiatives, these examples offer valuable insights into leveraging AI to address urban challenges and create smarter, more livable cities.

Adaptability to African Context

As African cities embark on smart city initiatives, several EU strategies offer adaptable frameworks that could address local cybersecurity challenges, resource constraints, and urban management needs. However, for successful adaptation, these strategies must account for Africa's unique socioeconomic landscape, regulatory environments, and technological infrastructure. Key areas where EU approaches might be adapted or modified for African contexts include:

1. **Data Protection and Privacy Frameworks**

   The EU's General Data Protection Regulation (GDPR) sets a high standard for data privacy, emphasizing the need for robust protections in digital services. While GDPR may be challenging to implement directly due to the varying legal and regulatory environments across Africa, its core principles, such as transparency, accountability, and individual rights over personal data, could be incorporated into data governance frameworks in African cities. Developing localized regulations that align with GDPR's privacy standards would help African cities manage data ethically, especially as IoT devices and AI tools increasingly collect and analyze sensitive information.

2. **Cross-Sectoral Cybersecurity Standards**

   The EU's Network and Information Security (NIS) Directive promotes cybersecurity collaboration across sectors, which

is crucial for African smart cities where public infrastructure and private tech sectors are closely intertwined. African cities can adopt similar cross-sectoral standards but tailor them to include local service providers and telecoms, as these entities often act as primary facilitators of connectivity in smart city projects. Additionally, creating partnerships with global cybersecurity bodies could provide African cities with knowledge-sharing and best practices, improving resilience against cyber threats despite limited local resources.

3. **Centralized Cybersecurity Agencies and Capacity Building**

The European Union Agency for Cybersecurity (ENISA) plays a central role in EU cyber resilience by setting guidelines and supporting member states with resources. African nations could benefit from establishing similar centralized agencies or regional collaborations focused on cybersecurity. These bodies would provide crucial cybersecurity guidance, facilitate the sharing of threat intelligence, and support training initiatives to address the continent's shortage of cybersecurity experts. By investing in training and certification programs, African cities could build local talent, thereby reducing reliance on external expertise and fostering a sustainable cybersecurity ecosystem.

4. **AI-Driven Public Service Optimization**

AI systems that streamline public services, such as Amsterdam's AI complaint analysis or Helsinki's parking chatbot, could be modified to meet African urban needs. For instance, AI could enhance urban waste management or optimize energy usage in African cities where these services are often under strain. Instead of focusing on high-cost infrastructure, African cities could begin with lower-cost AI implementations for essential services, like traffic management and utilities, aligning with local priorities and budgetary constraints. By integrating AI gradually, cities can benefit from increased efficiency without overextending their resources.

5. **Ethical AI Use and Socioeconomic Considerations**

Europe's value-driven approach to cybersecurity and AI, which aims to balance innovation with ethical considerations, provides a valuable blueprint for Africa. Adaptations could focus on ensuring that AI systems respect cultural contexts, language diversity, and digital inclusivity. Ethical AI policies could be tailored to prevent discrimination and promote equitable access across demographics, addressing Africa's unique challenges of urban inequality. African cities could also emphasize transparency and public awareness to build trust in AI and smart city technologies among residents, especially in communities where there may be concerns over surveillance or data use.

6. **Regional Collaboration on Cybersecurity**

African countries could also draw from the EU's model of regional collaboration to create a more unified approach to cybersecurity. Although Africa's diversity in regulatory and governance frameworks presents a challenge, regional bodies such as the African Union (AU) could coordinate cybersecurity standards, similar to how the EU addresses security across member states. Establishing shared cybersecurity protocols would help African cities respond more effectively to cross-border threats and facilitate knowledge-sharing, particularly through the harmonization of cyber policies and resources.

By carefully tailoring these EU strategies to the African context, African smart cities can adopt scalable, resilient, and ethically sound smart city models. This approach not only advances urban modernization but also fosters stronger regional cybersecurity infrastructures, helping African cities to thrive in an interconnected global environment.

CONCLUSION

To address the cybersecurity challenges in African smart cities, implementing AI-driven solutions requires a comprehensive approach that incorporates both practical strategies and supportive policies. As urban centers in Africa embrace technology, targeted

AI applications in data security, emergency response, and identity verification can directly respond to local security needs while addressing broader infrastructural constraints. One key area for development is data localization and privacy. Leveraging AI to manage data within national or regional boundaries offers a dual advantage: it bolsters data sovereignty and minimizes exposure to foreign cyber risks. Privacy-preserving AI methods, such as federated learning, can enhance data protection by analyzing local data without centralized storage, aligning with African data sovereignty goals.

To combat the prevalent issues in urban crime, real-time crime mapping and predictive analytics stand as critical AI tools. By integrating data from multiple sources, law enforcement databases, social media, and IoT sensor networks, AI systems can identify high-risk areas and project potential criminal activities. Implementing these systems, however, demands adaptation to local resources and infrastructure, particularly in cities where conventional law enforcement technologies may be sparse. A phased approach to deployment, starting with pilot projects in specific districts, can allow for adjustments and gradual scaling, ensuring the technology effectively integrates with existing urban management systems.

Moreover, AI can enhance emergency responsiveness in African cities by processing data from IoT sensors and coordinating urban systems, reducing response times and mitigating the impact of incidents. These demands dedicated regional AI innovation hubs, which can foster research, promote best practices, and develop applications tailored to local urban challenges. Such hubs, ideally backed by public-private partnerships, could accelerate AI adoption and serve as a collaborative base for testing and refining new technologies before widespread implementation. Alongside this, prioritizing skill development in AI and cybersecurity through dedicated knowledge-sharing networks can help address the shortage of AI talent across the continent. By organizing regional conferences, workshops, and virtual collaborations, cities can cultivate a pipeline of skilled professionals equipped to manage and expand AI applications.

For these AI implementations to be sustainable, African cities need a robust policy framework that emphasizes inclusivity and security. Governments can enhance public trust in AI by fostering transparency and community engagement, ensuring that AI governance reflects local societal values. Establishing inclusive AI standards and ethics councils can help create checks and balances, ensuring responsible use while addressing ethical concerns related to privacy and autonomy. Furthermore, open data policies that allow vetted access to anonymized public data can drive innovation, enabling AI applications to grow responsibly within a secure, transparent ecosystem. Finally, dedicated cybersecurity task forces within city administrations could streamline efforts across departments, creating a unified approach to urban cybersecurity.

In conclusion, African smart cities can effectively leverage AI-driven solutions by adopting adaptable, region-specific strategies that balance technological progress with data security, community engagement, and ethical governance. Establishing strong partnerships, fostering local AI expertise, and creating transparent policy structures will be crucial for cities aiming to build secure, resilient urban environments where AI plays a proactive role in public safety and data protection.

REFRENCES

[1]. Adomako, K., Mohamed, N., Garba, A.A., & Saint, M. (2018). Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index. *Social Science Research Network*.

[2]. Ahmad, I.A., Anyanwu, A.C., Onwusinkwue, S., Dawodu, S.O., Akagha, O.V., & Ejairu, E. (2024). CYBERSECURITY CHALLENGES IN SMART CITIES: A CASE REVIEW OF AFRICAN METROPOLISES. *Computer Science & IT Research Journal*.

[3]. Camacho, N.G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*.

[4]. Chen, D., Wawrzynski, P., & Lv, Z. (2020). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, 102655.

[5]. Dias, T., Fonseca, T., Vitorino, J., Martins, A.F., Malpique, S., & Praça, I. (2023). From Data to Action: Exploring AI and IoT-driven Solutions for Smarter Cities. *ArXiv, abs/2306.04653*.

[6]. Familoni, B.T. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. *Computer Science & IT Research Journal*.

[7]. Gracias, J.S., Parnell, G.S., Specking, E., Pohl, E.A., & Buchanan, R.K. (2023). Smart Cities—A Structured Literature Review. *Smart Cities*.

[8]. Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I., & Beer, J. (2020). Artificial Intelligence (AI) Deployments in Africa: Benefits, Challenges and Policy Dimensions.

[9]. Ilves, L.K., Evans, T.J., Cilluffo, F.J., & Nadeau, A.A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. *Prism: A Journal of the Center for Complex Operations, 6*, 126.

[10]. Jasmontaite, L., Fuster, G.G., Gutwirth, S., Wenger, F., Jaquet-Chiffelle, D., & Schlehahn, E. (2017). Canvas White Paper 2 – Cybersecurity and Law. *Social Science Research Network*.

[11]. Khafif, M.K., & Salem, N. (2021). Smart Cities - Policy and Regulatory Frameworks. *Design and Construction of Smart Cities*.

[12]. Li, J. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering, 19*, 1462-1474.

[13]. Mark, R., & Anya, G. (2019). Ethics of Using Smart City AI and Big Data: The Case of Four Large European Cities. *The ORBIT Journal*.

[14]. Nibigira, N., Havyarimana, V., & Xiao, Z. (2024). Artificial Intelligence Adoption for Cybersecurity in Africa. *Journal of Information Security*.

[15]. Oliha, J.S., Biu, P.W., & Obi, O.C. (2024). SECURING THE SMART CITY: A REVIEW OF CYBERSECURITY CHALLENGES AND STRATEGIES. *Engineering Science & Technology Journal*.

[16]. Orji, U.J. (2012). The defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity. *2012 Third Worldwide Cybersecurity Summit (WCS)*, 1-7.

[17]. Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*.

[18]. Romaniuk, S.N., Fotescu, A., & Chihaia, M.S. (2020). NATO's evolving cyber security policy and strategy.

[19]. Ruohonen, J. (2019). An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union. *European Journal for Security Research, 5*, 349 - 377.

[20]. Salceda, J.V., Napagao, S.Á., Gómez, J.A., Felipe, L.J., Gasulla, D.G., Sebastià, I.G., & Busquet, V.C. (2014). Making smart cities smarter using artificial intelligence techniques for smarter mobility. *International Conference on Smart Grids and Green IT Systems*.

[21]. Sarker, I.H., Furhad, M.H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science, 2*.

[22]. Škundrić, P., Korać, V., & Davidovac, Z. (2022). EU Cyber Initiatives and International Cybersecurity Standards — An Overview. *Arheologija i prirodne nauke*.

[23]. Stefanouli, M., & Economou, C. (2018). Data Protection in Smart Cities: Application of the EU GDPR. *Data Analytics: Paving the Way to Sustainable Urban Mobility*.

[24]. Turianskyi, Y. (2018). Balancing Cyber Security and Internet Freedom in Africa.

[25]. Vandercruysse, L., Buts, C., & Dooms, M. (2020). A typology of Smart City services: The case of Data Protection Impact Assessment. *Cities*.

[26]. Vázquez-Salceda, J. (2014). Making Smart Cities Smarter - Using Artificial Intelligence Techniques for Smarter Mobility. *International Conference on Smart Grids and Green IT Systems*.