OPEN ACCESS
Computer Science & IT Research Journal
P-ISSN: 2709-0043, E-ISSN: 2709-0051
Volume 5, Issue 2, P.254-269, February 2024
DOI: 10.51594/csitrj.v5i2.756
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/csitrj

CYBERSECURITY CHALLENGES IN SMART CITIES: A CASE REVIEW OF AFRICAN METROPOLISES

Islam Ahmad Ibrahim Ahmad[1], Anthony Chigozie Anyanwu[2], Shedrack Onwusinkwue[3], Samuel Onimisi Dawodu[4], Onyinyechi Vivian Akagha[5], & Emuesiri Ejairu[6]

[1]Independent Researcher, Plano, TX, U.S.A
[2]Independent Researcher, San Francisco, USA
[3]Department of Physics, University of Benin, Nigeria
[4]NDIC, Nigeria
[5]Independent Researcher, Ireland
[6]Independent Researcher, Indiana, U.S.A

*Corresponding Author: Samuel Onimisi Dawodu
Corresponding Author Email: Dawodu_sam@yahoo.com
Article Received: 30-11-23 **Accepted:** 20-01-24 **Published:** 02-02-24

ABSTRACT

The rapid urbanization and digital transformation of cities across Africa have given rise to the concept of Smart Cities, where advanced technologies are integrated to enhance efficiency, sustainability, and the overall quality of urban life. However, this paradigm shift towards interconnected and technology-driven urban environments brings forth a host of cybersecurity challenges that demand careful consideration. This paper explores the cybersecurity challenges in Smart Cities, focusing on a case review of African metropolises. African cities, emblematic of the global urbanization trend, are embracing Smart City initiatives to address urban challenges and

foster economic development. While these initiatives promise improved services and enhanced connectivity, they concurrently expose cities to a myriad of cybersecurity threats. The interconnectedness of devices and systems in Smart Cities creates a vast attack surface, making them susceptible to cyber-attacks ranging from data breaches to infrastructure disruptions. This case review delves into specific instances of cybersecurity challenges faced by African metropolises in their quest for technological advancement. It analyzes the vulnerabilities in critical infrastructure, such as energy grids, transportation systems, and healthcare networks, highlighting the potential risks associated with inadequate cybersecurity measures. Moreover, the paper sheds light on the socio-economic implications of cyber threats in Smart Cities, emphasizing the importance of resilient cybersecurity frameworks in safeguarding citizen data and urban functionality. In conclusion, the paper underscores the urgent need for comprehensive cybersecurity strategies tailored to the unique challenges faced by Smart Cities in Africa. The findings aim to contribute to a better understanding of the intricate relationship between urbanization, technology, and cybersecurity, offering insights that can inform policy decisions, technological implementations, and collaborative efforts to build secure and resilient Smart Cities in the African context.

Keywords: Cybersecurity, Smart Cities, Africa, Metropolis, Review.

INTRODUCTION

As the world witnesses unprecedented urbanization and technological advancements, the concept of Smart Cities has emerged as a transformative solution to address the complex challenges faced by urban environments (Paiva *et al*., 2021). Smart Cities leverage cutting-edge technologies to enhance the efficiency of urban services, improve resource utilization, and elevate the overall quality of life for citizens (Alahi *et al*., 2023). However, as these cities integrate various technological components, they become vulnerable to cybersecurity threats that can have far-reaching consequences (Almeida, 2023). This scientific paper aims to explore the cybersecurity challenges inherent in Smart Cities, with a specific focus on African metropolises undergoing rapid digital transformations.

Smart Cities represent a paradigm shift in urban development, where Information and Communication Technologies (ICT) are seamlessly integrated to optimize infrastructure, services, and communication (Mohanty and Kumar, 2021). These cities utilize interconnected sensors, devices, and systems to collect and analyze data, allowing for real-time decision-making and resource management (Ramírez-Moreno *et al*, 2021). The goal is to create cities that are sustainable, resilient, and responsive to the needs of their inhabitants. Smart Cities encompass a wide range of sectors, including transportation, energy, healthcare, and governance, all interconnected through a sophisticated digital infrastructure (Ahad *et al*., 2020).

In the African context, the significance of Smart City initiatives is particularly pronounced as these metropolises grapple with the challenges of rapid urbanization, resource constraints, and the need for sustainable development. The implementation of Smart City technologies in African cities holds the promise of addressing longstanding issues such as traffic congestion, inadequate

healthcare, and inefficient resource management (Boyle *et al*., 2023). Moreover, it presents an opportunity for leapfrogging traditional developmental stages, allowing African cities to embrace innovation and technology for accelerated growth.

The integration of technology in urban environments is a multifaceted process that involves the deployment of IoT (Internet of Things) devices, sensors, and advanced communication networks (Nižetić *et al*., 2020). Smart Cities use data analytics and artificial intelligence to gather insights from various sources, enabling predictive modeling and efficient resource allocation (Olaniyi *et al*., 2023). For instance, smart transportation systems utilize real-time data to optimize traffic flow and reduce congestion, while smart energy grids enhance sustainability by optimizing energy distribution. In healthcare, the integration of technology enables remote monitoring and personalized healthcare services (Mbunge *et al*., 2021).

The interconnected nature of these technologies facilitates seamless communication between different components of the urban infrastructure, providing a holistic view of the city's functioning (Mishra and Singh, 2023). While these advancements promise substantial benefits, they also expose Smart Cities to a new set of challenges, particularly in the realm of cybersecurity.

As Smart Cities become the focal point of urban development in Africa, the cybersecurity challenges they face demand careful examination (Demertzi *et al*., 2023). The interconnectedness of devices and systems in these cities creates an expansive attack surface, making them susceptible to a range of cyber threats (Demertzi *et al*., 2023). This paper contends that the cybersecurity challenges in Smart Cities, especially in the African context, require focused attention and innovative solutions. Through a case review of representative African metropolises, we aim to identify specific instances of cybersecurity vulnerabilities and their socio-economic implications. Furthermore, the paper seeks to contribute insights that can inform the development of robust cybersecurity strategies tailored to the unique challenges faced by Smart Cities in Africa.

Smart City initiatives in Africa

The emergence of Smart City initiatives in Africa can be traced back to the early 21st century when the continent witnessed a surge in urbanization and a growing need for innovative solutions to address urban challenges (Bandauko and Nutifafa Arku, 2023). African governments and municipalities, cognizant of the potential of technology to transform urban living, began embracing the concept of Smart Cities. The initial focus was on leveraging information and communication technologies (ICT) to enhance governance, infrastructure, and service delivery (Uyar *et al*., 2021).

One of the pioneering efforts in this regard was the implementation of the Smart Cape initiative in Cape Town, South Africa, in the mid-2000s (Turok *et al*., 2021). The project aimed to use technology to improve public services, enhance safety, and boost economic development. Following this, other major African cities, including Nairobi, Lagos, and Cairo, started exploring Smart City concepts, realizing the need for sustainable urban development in the face of rapid population growth.

In subsequent years, the African Union's Agenda 2063, a strategic framework for the socio-economic transformation of the continent, highlighted the importance of harnessing technology for

urban development. This emphasis on technology as a catalyst for progress laid the foundation for more comprehensive Smart City initiatives across the continent.

The integration of technology into Smart Cities involves a diverse range of cutting-edge innovations that collectively contribute to the development of intelligent urban environments. Among the key technologies integrated into Smart Cities in Africa are Internet of Things (IoT) plays a pivotal role in Smart Cities by connecting physical devices and sensors to the internet, enabling them to collect and exchange data. This connectivity allows for real-time monitoring and management of various aspects of urban life, such as traffic flow, energy consumption, and waste management. The use of big data analytics enables Smart Cities to process vast amounts of information collected from IoT devices. This data-driven approach facilitates informed decision-making, predictive modeling, and the identification of patterns that can optimize urban services and infrastructure. AI technologies, including machine learning and natural language processing, contribute to the automation of processes and the development of intelligent systems (Sarker, 2022, Anamu et al., 2023, Mouchou et al., 2021, Sanni et al., 2024). In Smart Cities, AI is employed in areas such as traffic management, public safety, and healthcare to enhance efficiency and responsiveness. This includes the integration of advanced technologies into traditional urban infrastructure. Smart grids enhance energy efficiency, intelligent transportation systems reduce traffic congestion, and smart buildings incorporate energy-saving features and automation for improved sustainability. The convergence of physical infrastructure with digital technologies results in cyber-physical systems (Bordoloi *et al*., 2022). These systems, encompassing smart grids, smart transportation, and smart healthcare, create a cohesive and interconnected urban environment.

Smart Cities hold immense promise for African metropolises, offering a range of potential benefits that address pressing urban challenges and contribute to sustainable development. Through the deployment of smart technologies, cities can optimize the use of resources such as energy, water, and transportation. This efficiency not only reduces costs but also contributes to environmental sustainability. Smart City initiatives aim to enhance the overall quality of life for residents. This involves the provision of better healthcare services, efficient public transportation, and the creation of safer and more secure urban environments. The integration of technology stimulates economic growth by attracting investment, fostering innovation, and creating job opportunities. Smart Cities become hubs for technological advancements, leading to increased competitiveness on the global stage (Rani *et al*., 2021). Smart Cities leverage digital connectivity to create a seamless and interconnected urban experience. Residents benefit from improved communication, accessibility to services, and real-time information on various aspects of city life. With a focus on smart infrastructure and sustainable practices, Smart Cities contribute to environmental conservation. Reduced energy consumption, waste management optimization, and green initiatives make these cities ecologically responsible (Almalki *et al*., 2023).

In conclusion, the history of Smart City initiatives in Africa reflects a strategic response to the challenges of urbanization and a commitment to leveraging technology for sustainable development. The integration of key technologies not only signifies progress but also introduces a

new set of challenges, particularly in the realm of cybersecurity. Understanding the historical context and the potential benefits of Smart Cities sets the stage for a comprehensive examination of the cybersecurity challenges faced by African metropolises undergoing digital transformations (Bibri *et al*., 2024).

Cybersecurity Landscape in Smart Cities

The rapid proliferation of Smart Cities introduces a new dimension to the traditional cybersecurity landscape, demanding a paradigm shift in strategies and approaches. Urban environments, characterized by interconnected systems and a multitude of devices, present a complex web of vulnerabilities that cyber threats can exploit (Stellios *et al*., 2022). The conventional focus on securing individual computers and networks must now expand to safeguarding entire city infrastructures.

In the context of Smart Cities, cybersecurity extends beyond protecting personal data to ensuring the reliability and security of critical urban systems (Rizi and Seno, 2022). This includes transportation networks, energy grids, healthcare services, and governance mechanisms, all of which are increasingly reliant on interconnected technologies. The interconnected nature of these systems amplifies the potential impact of cyber threats, making them more pervasive and potentially devastating.

The integration of Internet of Things (IoT) devices and sensors across diverse urban sectors vastly expands the attack surface for potential cyber threats. Each connected device becomes a potential entry point, making it challenging to monitor and secure the entire network comprehensively as explain in figure 1.

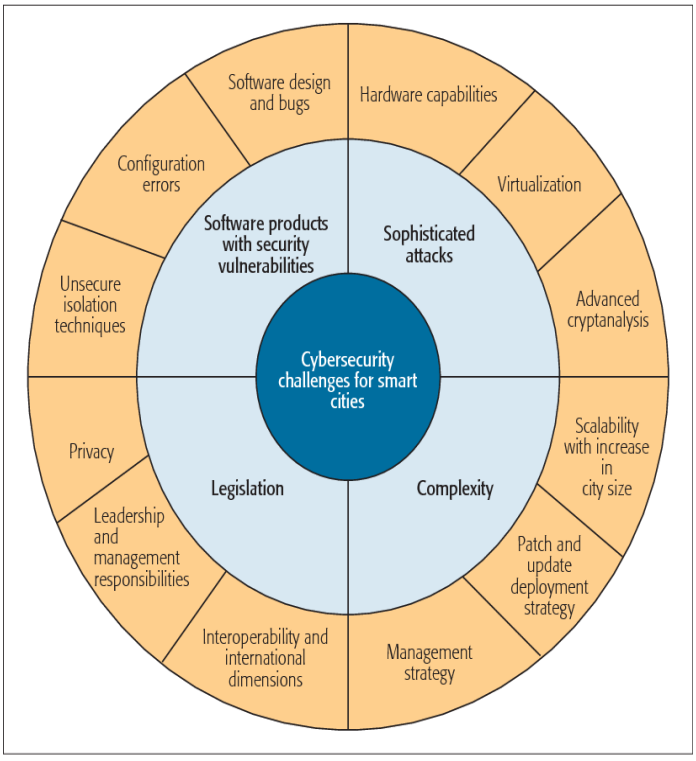

Figure 1. Cybersecurity Challenges for Smart Cities (Khatoun and Zeadally, 2017)

Smart Cities operate as intricate webs of interdependent systems. A cyber-attack on one component can have cascading effects on others, leading to disruptions in essential services (Palleti *et al*., 2021). For instance, a breach in the transportation system may affect emergency services, exacerbating the impact of the attack.

The extensive collection and analysis of data in Smart Cities raise significant concerns about privacy. The interconnectedness of systems can lead to the aggregation of sensitive information, and any compromise in data security may have severe implications for citizen privacy and trust in the system (Atlam and Wills, 2020). Many Smart Cities integrate advanced technologies into existing, often legacy, infrastructure. This integration poses challenges as legacy systems may have vulnerabilities that are difficult to address, potentially serving as weak links in the overall cybersecurity framework. The human element remains a vulnerability in the Smart City cybersecurity landscape. From city administrators to citizens, the susceptibility to phishing attacks, social engineering, and negligent security practices can compromise the integrity of the entire system.

Trust is paramount in the successful implementation of Smart City initiatives. The public must have confidence that their data is secure, and the services they rely on are resilient to cyber threats. A breach of this trust not only undermines the success of Smart Cities but also erodes public confidence in digital governance. The functionality of Smart City infrastructure is crucial for maintaining economic and operational stability. Cyberattacks on critical systems can disrupt services, leading to economic losses, compromised public safety, and a breakdown of essential urban functions (Avraam *et al*., 2023). Smart Cities are integral components of national infrastructure, and their compromise can have far-reaching national security implications. Cyberattacks targeting critical urban systems may not only disrupt city functions but also pose threats at a broader geopolitical level. Smart Cities collect and process vast amounts of sensitive data, ranging from personal information to critical infrastructure details (Ismagilova *et al*., 2020). Ensuring the confidentiality, integrity, and availability of this data is imperative to prevent unauthorized access, data breaches, and potential misuse. The dynamic nature of cyber threats necessitates a proactive and adaptive cybersecurity approach. Smart Cities must continuously evolve their cybersecurity strategies to address emerging threats, vulnerabilities, and attack vectors, ensuring resilience against evolving cyber risks (Nova, 2022).

In conclusion, the cybersecurity landscape in Smart Cities is a critical aspect of their success and sustainability. The interconnected nature of urban systems introduces unique challenges that require innovative and comprehensive solutions. As Smart Cities continue to evolve, the importance of robust cybersecurity measures cannot be overstated. The proactive protection of critical infrastructure, sensitive data, and public trust is essential to realizing the promise and potential benefits of Smart Cities in the digital age (Demertzi *et al*., 2023). Addressing these challenges head-on will not only secure the urban environments of today but also pave the way for the resilient and secure cities of the future.

Case Review of African Metropolises

Across the African continent, several metropolises have embarked on ambitious Smart City initiatives to harness the potential of technology for urban development (Agunbiade *et al*., 2021). Notable among them are Johannesburg (South Africa), Nairobi (Kenya), Lagos (Nigeria), and Cairo (Egypt). These cities represent diverse economic, cultural, and demographic contexts, offering a comprehensive view of the challenges and opportunities associated with Smart City transformations in Africa.

In Johannesburg, a critical financial hub in South Africa, vulnerabilities in the smart transportation system were exploited in a cyber-attack, leading to disruptions in traffic management and public transportation services (Ding *et al*., 2022). The interconnected nature of the city's transportation grid allowed the attackers to infiltrate and manipulate traffic signals, causing congestion and potential safety hazards. This incident exposed the susceptibility of essential infrastructure to cyber threats, emphasizing the need for robust security measures in critical urban systems.

Nairobi, a rapidly growing city in East Africa, faced a significant data breach in its smart healthcare system. Personal health records of citizens were compromised, raising serious privacy concerns. The breach not only jeopardized sensitive medical information but also eroded public trust in the healthcare services provided by the Smart City initiative (Okafor *et al*., 2023). This case underscores the importance of securing data repositories and ensuring stringent privacy measures to protect citizen information.

Lagos, a sprawling metropolis in Nigeria, experienced a cyber-attack that targeted the smart governance systems. The attackers disrupted online municipal services, including citizen portals for permits and licenses. This not only hindered routine administrative processes but also had socio-economic implications as businesses and individuals faced delays and uncertainties. The incident highlighted the interconnectedness of administrative services in Smart Cities and the potential socio-economic repercussions of cybersecurity breaches.

One of the root causes identified is the insufficient investment in cybersecurity infrastructure. Many African Smart Cities are still developing their cybersecurity capabilities, leading to vulnerabilities in the face of increasingly sophisticated cyber threats (Soare and Burton, 2020). The lack of comprehensive cybersecurity frameworks and skilled professionals exacerbates the challenges faced by these cities.

The rapid adoption of Smart City technologies without meticulous planning contributes to cybersecurity challenges (Javed *et al*., 2022). Cities often integrate advanced technologies into existing infrastructures without adequately assessing vulnerabilities, creating an environment where legacy systems may become points of weakness susceptible to cyber-attacks.

A notable factor contributing to cybersecurity challenges is the insufficient awareness and training of both city administrators and citizens. Without a well-informed user base, Smart City initiatives become more susceptible to human-centric vulnerabilities, such as social engineering attacks and negligent security practices (Iqbal and Olariu, 2020).

The absence of standardized security protocols across African Smart Cities further compounds cybersecurity challenges. Each city may adopt different technologies and security measures, making it challenging to establish cohesive defense strategies and collaborate on threat intelligence. Limited collaboration and information sharing among African Smart Cities hinder the collective response to cybersecurity threats (Mishra and Singh, 2023). Establishing regional or continental alliances for sharing threat intelligence and best practices could enhance the cybersecurity posture of individual cities.

In conclusion, the case review of African metropolises undergoing Smart City transformations reveals a nuanced landscape of cybersecurity challenges. The vulnerabilities in critical infrastructure, data breaches, and socio-economic impacts highlight the multifaceted nature of the threats faced by these cities. Addressing the root causes, such as limited cybersecurity infrastructure, rapid technological adoption without robust planning, inadequate awareness and training, lack of standardized security protocols, and insufficient collaboration, is imperative for building resilient and secure Smart Cities in Africa (Djenna *et al*., 2021). The findings from this case review emphasize the need for strategic investments, comprehensive planning, and collaborative efforts to mitigate cybersecurity risks and ensure the sustainable development of Smart Cities across the continent.

Socio-Economic Implications

The pervasive nature of cybersecurity threats in Smart Cities extends beyond technical disruptions, with profound socio-economic implications that can reverberate throughout urban communities (Fjäder, 2022). As cities increasingly rely on interconnected systems and digital infrastructure, the consequences of cyber threats extend to various facets of daily life.

Cybersecurity threats can lead to the disruption of essential urban services, impacting sectors such as transportation, healthcare, and energy distribution (Osei-Kyei *et al*., 2021). For instance, an attack on smart transportation systems may result in traffic chaos, affecting daily commuting patterns and hindering the movement of goods and services. Disruptions in healthcare systems can compromise patient care and public health, emphasizing the critical importance of secure and resilient services.

The economic implications of cybersecurity threats are significant. Downtime and disruptions caused by attacks on Smart City infrastructure can result in substantial economic losses (Avraam *et al*., 2023). Businesses may face interruptions in operations, supply chains can be disrupted, and productivity may decline. These economic repercussions extend beyond individual enterprises to impact the overall economic stability of the city and its ability to attract investment.

The economic fallout from cybersecurity threats in Smart Cities is multifaceted. Direct financial losses due to system downtime, data breaches, and the costs associated with cybersecurity recovery measures can cripple businesses and municipal budgets (Huang and Wang, 2021). Furthermore, the tarnished reputation of a city as an unsafe or unreliable digital environment may deter potential investors and hinder economic growth. A city's ability to foster innovation and attract tech-driven industries can be severely hampered by the perception of vulnerability to cyber threats.

Societal impacts are pronounced as cybersecurity threats can compromise citizen safety and well-being. For example, attacks on smart surveillance systems or emergency response mechanisms can impede the city's ability to address public safety concerns effectively. Additionally, data breaches that expose personal information can erode public trust in Smart City initiatives, leading to reluctance in adopting digital services and technology.

The political implications of cybersecurity threats are evident in the potential erosion of public confidence in government authorities (Shandler and Gomez, 2023). Leaders may face scrutiny for inadequate cybersecurity measures, and their ability to govern effectively may be questioned. The fallout from cyber incidents can become a political issue, influencing public opinion and potentially shaping electoral outcomes. The political landscape may also be impacted by the need for swift and effective responses to cyber threats, requiring policymakers to prioritize cybersecurity on their agendas (Kayode-Ajala, 2023).

A crucial aspect of the socio-economic impact of cybersecurity threats is the erosion of citizen trust. In Smart Cities, where digital interactions are integral to daily life, any compromise in cybersecurity can lead to a loss of faith in the reliability and security of digital services. Restoring trust requires transparent communication, robust security measures, and citizen engagement to ensure that the urban community remains actively involved in the process of securing the city's digital infrastructure (Xia *et al*., 2023).

Cybersecurity threats can exacerbate existing socio-economic disparities, as vulnerable populations may be disproportionately affected. For instance, disruptions in digital services can hinder access to critical resources and information, impacting marginalized communities more severely. Ensuring equity in cybersecurity measures and promoting accessibility to secure digital services is essential for fostering an inclusive and resilient urban environment.

Building resilience against cybersecurity threats requires collaborative responses from urban communities. Encouraging citizens to be vigilant, practice good cyber hygiene, and actively participate in community-wide cybersecurity initiatives is crucial. Community awareness programs, educational campaigns, and the inclusion of diverse voices in the planning and implementation of Smart City cybersecurity measures can enhance the overall security posture of the city (Marchesani, 2023).

In conclusion, the socio-economic implications of cybersecurity threats in Smart Cities extend far beyond technical disruptions. The economic, social, and political ramifications underscore the interconnectedness of cybersecurity with the fabric of urban life. A holistic understanding of these implications is imperative for policymakers, city administrators, and citizens alike (Marschütz *et al*., 2020). By addressing the socio-economic impacts of cybersecurity threats, cities can cultivate resilience, foster economic growth, and ensure that the benefits of Smart City initiatives are realized across diverse urban communities.

Cybersecurity Strategies for Smart Cities in Africa

The cybersecurity landscape in Smart Cities across Africa is evolving, with several cities grappling with the challenges of securing complex, interconnected urban systems (Adel, 2023). While some countries have made strides in developing cybersecurity frameworks and policies, there is a need

for a comprehensive examination of existing initiatives to identify gaps and areas for improvement.

Some African countries have formulated national cybersecurity strategies that provide a high-level framework for securing digital infrastructure. These strategies typically outline the government's commitment to cybersecurity, establish regulatory frameworks, and delineate roles and responsibilities. However, the effectiveness of these strategies often depends on their implementation and adaptation to the unique challenges posed by Smart Cities.

Data protection and privacy laws are critical components of cybersecurity frameworks. Many African countries have enacted or are in the process of formulating legislation to protect citizen data and privacy. However, the enforcement of these laws and their relevance to the dynamic nature of Smart City technologies require continual assessment and adaptation (Xia *et al*., 2023).

Some countries have implemented sector-specific regulations addressing cybersecurity concerns in critical infrastructure sectors. These regulations may cover areas such as energy, transportation, and healthcare. However, the integration of these regulations into the broader Smart City context is crucial for a cohesive and effective cybersecurity strategy.

Conducting comprehensive risk assessments is fundamental to understanding the threat landscape and vulnerabilities within Smart Cities (Nova, 2022). This involves identifying potential risks, evaluating their impact on critical infrastructure, and prioritizing areas for cybersecurity investment and improvement.

Smart Cities in Africa can benefit from adopting international cybersecurity standards and best practices. Standards such as ISO/IEC 27001 for information security management and NIST Cybersecurity Framework provide a solid foundation for developing robust cybersecurity measures. Aligning with these standards ensures a globally recognized and interoperable approach to cybersecurity.

Building local capacity in cybersecurity skills is crucial for implementing and maintaining effective cybersecurity measures. Investing in training programs, workshops, and educational initiatives can empower local talent to address the unique challenges of Smart Cities (Tan and Taeihagh, 2020). This includes training cybersecurity professionals, city administrators, and even the general public to enhance overall cyber hygiene.

Establishing robust monitoring mechanisms is essential for early detection of cyber threats. Implementing advanced monitoring tools, threat intelligence sharing, and real-time incident response capabilities enable Smart Cities to react swiftly to emerging threats, minimizing the potential impact of cybersecurity incidents.

Integrating cybersecurity into the design phase of Smart City projects is critical. Adhering to secure-by-design principles ensures that cybersecurity considerations are embedded in the development and implementation of technologies, preventing vulnerabilities that may be exploited in the future (Chattopadhyay *et al*., 2020).

Collaboration between governments and the private sector is essential for effective cybersecurity in Smart Cities. Establishing public-private partnerships fosters information sharing, joint threat intelligence efforts, and coordinated responses to cyber incidents. This collaboration leverages the

expertise and resources of both sectors for a more comprehensive and resilient cybersecurity strategy.

Involving cybersecurity experts and industry stakeholders is crucial for staying ahead of evolving cyber threats. Governments and Smart City initiatives should engage with the cybersecurity industry to access the latest technologies, threat intelligence, and expertise (Kitchin and Dodge, 2020). This collaboration ensures that Smart Cities can proactively address emerging cybersecurity challenges.

Cyber threats often transcend national borders, making cross-border collaboration imperative. African Smart Cities should engage in regional and international collaboration to share threat intelligence, best practices, and lessons learned. Cross-border collaboration enhances the collective cybersecurity resilience of Smart Cities and contributes to a more secure digital environment.

In addition to governments and the private sector, involving multiple stakeholders such as academia, civil society, and local communities is crucial. This multi-stakeholder approach ensures diverse perspectives, fosters innovation, and promotes inclusivity in developing and implementing cybersecurity strategies for Smart Cities (Anthony, 2022).

In conclusion, securing Smart Cities in Africa requires a holistic approach that addresses existing cybersecurity frameworks, incorporates recommendations for resilience, and emphasizes collaboration between governments, the private sector, and cybersecurity experts. By examining and enhancing existing strategies, Smart Cities can navigate the evolving cybersecurity landscape, mitigate risks, and create a foundation for sustainable and secure digital urban environments. The collaborative efforts of all stakeholders will play a pivotal role in building resilient Smart Cities that thrive in the face of cybersecurity challenges (Rhee, 2020).

RECOMMENDATION AND CONCLUSION

The case review of African metropolises undergoing Smart City transformations has unearthed critical insights into the cybersecurity challenges faced by these urban environments. Across representative cities such as Johannesburg, Nairobi, Lagos, and Cairo, vulnerabilities in critical infrastructure, data breaches, and socio-economic impacts were identified as recurring themes. The examination highlighted the intricate web of interconnected systems, the potential consequences of cyber threats on essential services, and the broader implications for economic stability, social trust, and political resilience.

The urgency for robust cybersecurity measures in Smart Cities cannot be overstated. The interconnected nature of urban systems, coupled with the increasing sophistication of cyber threats, necessitates immediate and comprehensive action. The case review underscores that cybersecurity is not merely a technical concern but a fundamental prerequisite for the success and sustainability of Smart City initiatives. The potential economic losses, disruptions in critical services, and erosion of public trust emphasize the critical need for cities to prioritize and invest in cybersecurity resilience.

In light of the findings, a collective call to action is essential for all stakeholders involved in the development and governance of Smart Cities in Africa. This includes government bodies, private

sectors, academia, cybersecurity experts, and local communities. The following actions are recommended:

Governments and private sectors should allocate substantial resources to build and enhance cybersecurity infrastructure in Smart Cities. This involves investing in advanced technologies, training cybersecurity professionals, and implementing robust monitoring and incident response mechanisms. The potential gains from embracing connected smart cities are great, but they come entangled with great responsibilities and risks.

Governments need to continuously review and update existing cybersecurity policies to align with the evolving threat landscape of Smart Cities. These policies should encompass data protection, privacy laws, and sector-specific regulations, providing a comprehensive framework for securing critical infrastructure. These policies must adapt and change in the speed of technology.

A concerted effort is needed to raise public awareness about cybersecurity threats and best practices. Educational campaigns targeting citizens, businesses, and government employees can foster a culture of cybersecurity awareness and responsibility. Informed individuals are more likely to contribute to the overall resilience of Smart Cities. And this shall improve the future of the society and the country overall. A more educated and informed public will help improvement efforts.

Smart Cities in Africa should actively engage in international collaboration and information sharing to stay abreast of global cybersecurity trends. Learning from the experiences of other cities and leveraging international partnerships can enhance the effectiveness of cybersecurity strategies.

Governments, private sectors, academia, and local communities should collaboratively develop and implement cybersecurity strategies. Involving diverse stakeholders ensures a holistic approach that considers the unique challenges faced by Smart Cities and facilitates innovation and knowledge-sharing.

Smart Cities should adopt a proactive stance towards cybersecurity by continuously monitoring the threat landscape and adapting their strategies accordingly. Regular assessments, penetration testing, and scenario-based exercises can help cities stay one step ahead of cyber threats. Local policies are more agile and tuned with the needs of their society.

In conclusion, the case review of cybersecurity challenges in African metropolises has provided a foundation for urgent and decisive action. The recommendations underscore the imperative for immediate investments, policy revisions, public awareness campaigns, and collaborative efforts to fortify the cybersecurity resilience of Smart Cities. The call to action is not just a suggestion but a collective responsibility to safeguard the digital infrastructure, economic stability, and societal well-being of African metropolises in the era of rapid urbanization and technological advancement. By heeding this call, stakeholders can contribute to the creation of Smart Cities that thrive securely, fostering innovation, inclusivity, and sustainable urban development.

Reference

Adel, A. (2023). Unlocking the future: fostering human–machine collaboration and driving intelligent automation through industry 5.0 in smart cities. *Smart Cities*, *6*(5), 2742-2782.

Agunbiade, M.E., Olajide, O., & Bishi, H. (2021). Urban governance and smart future cities in Nigeria: Lagos flagship projects as springboard?. *Refractions of the National, the Popular and the Global in African Cities*, 127.

Ahad, M.A., Paiva, S., Tripathi, G., & Feroz, N. (2020). Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*, *61*, 102301.

Alahi, M.E.E., Sukkuea, A., Tina, F.W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S.C. (2023). Integration of IoT-Enabled technologies and artificial intelligence (ai) for smart city scenario: recent advancements and future trends. *Sensors*, *23*(11), 5206.

Almalki, F.A., Alsamhi, S.H., Sahal, R., Hassan, J., Hawbani, A., Rajput, N.S., Saif, A., Morgan, J., & Breslin, J. (2023). Green IoT for eco-friendly and sustainable smart cities: future directions and opportunities. *Mobile Networks and Applications*, *28*(1), 178-202.

Almeida, F. (2023). Prospects of cybersecurity in smart cities. *Future Internet*, *15*(9), 285.

Anamu, U.S., Ayodele, O.O., Olorundaisi, E., Babalola, B.J., Odetola, P.I., Ogunmefun, A., Ukoba, K., Jen, T.C., & Olubambi, P.A. (2023). Fundamental design strategies for advancing the development of high entropy alloys for thermo-mechanical application: A critical review. *Journal of Materials Research and Technology*.

Anthony Jnr, B. (2022). Exploring data driven initiatives for smart city development: empirical evidence from techno-stakeholders' perspective. *Urban Research & Practice*, *15*(4), 529-560.

Atlam, H.F., & Wills, G.B. (2020). IoT security, privacy, safety and ethics. *Digital Twin Technologies and Smart Cities*, 123-149.

Avraam, C., Ceferino, L., & Dvorkin, Y. (2023). Operational and economy-wide impacts of compound cyber-attacks and extreme weather events on electric power networks. *Applied Energy*, *349*, 121577.

Avraam, C., Ceferino, L., & Dvorkin, Y. (2023). Operational and economy-wide impacts of compound cyber-attacks and extreme weather events on electric power networks. *Applied Energy*, *349*, 121577.

Bandauko, E., & Nutifafa Arku, R. (2023). A critical analysis of 'smart cities' as an urban development strategy in Africa. *International Planning Studies*, *28*(1), 69-86.

Bibri, S.E., Krogstie, J., Kaboli, A., & Alahi, A. (2024). Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. *Environmental Science and Ecotechnology*, *19*, 100330.

Bordoloi, T., Shapira, P., & Mativenga, P. (2022). Policy interactions with research trajectories: The case of cyber-physical convergence in manufacturing and industrials. *Technological Forecasting and Social Change*, *175*, 121347.

Boyle, L., Harlow, J., & Keeler, L.W. (2023). (D) evolving smartness: exploring the changing modalities of smart city making in Africa. *Urban Geography*, 1-25.

Chattopadhyay, A., Lam, K.Y., & Tavva, Y. (2020). Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems*, *22*(11), 7015-7029.

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Applied Sciences*, *13*(2), 790.

Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, *15*(18), 6799.

Djenna, A., Harous, S., & Saidouni, D.E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.

Fjäder, C. (2022). Emerging and disruptive technologies and security: considering trade-offs between new opportunities and emerging risks. In *Disruption, Ideation and Innovation for Defence and Security* (pp. 51-75). Cham: Springer International Publishing.

Huang, H.H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, *96*(3), 261-286.

Iqbal, A., & Olariu, S. (2020). A survey of enabling technologies for smart communities. *Smart Cities*, *4*(1), 54-77.

Ismagilova, E., Hughes, L., Rana, N.P., & Dwivedi, Y.K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.

Javed, A.R., Shahzad, F., ur Rehman, S., Zikria, Y.B., Razzak, I., Jalil, Z., & Xu, G. (2022). Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. *Cities*, *129*, 103794.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51-59.

Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In *Smart Cities and Innovative Urban Technologies* (pp. 47-65). Routledge.

Marchesani, F. (2023). Navigating the smart cities: conclusions and final remarks. In *The Global Smart City* (pp. 137-159). Emerald Publishing Limited.

Marschütz, B., Bremer, S., Runhaar, H., Hegger, D., Mees, H., Vervoort, J., & Wardekker, A. (2020). Local narratives of change as an entry point for building urban climate resilience. *Climate Risk Management*, *28*, 100223.

Mbunge, E., Muchemwa, B., & Batani, J. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. *Global Health Journal*, *5*(4), 169-177.

Mishra, P., & Singh, G. (2023). Energy management systems in sustainable smart cities based on the internet of energy: A technical review. *Energies*, *16*(19), 6903.

Mohanty, R., & Kumar, B.P. (2021). Urbanization and smart cities. In *Solving urban infrastructure problems using smart city technologies* (pp. 143-158). Elsevier.

Mouchou, R., Laseinde, T., Jen, T.C., & Ukoba, K. (2021). Developments in the application of nano materials for photovoltaic solar cell design, based on industry 4.0 integration scheme. In Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2021 Virtual Conferences on Human Factors in Software and Systems Engineering, Artificial Intelligence and Social Computing, and Energy, July 25-29, 2021, USA (pp. 510-521). Springer International Publishing.

Nižetić, S., Šolić, P., Gonzalez-De, D.L.D.I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877.

Nova, K. (2022). Security and resilience in sustainable smart cities through cyber threat intelligence. *International Journal of Information and Cybersecurity*, *6*(1), 21-42.

Okafor, C.M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N.L., Onunka, O., & Omotosho, A. (2023). Mitigating cybersecurity risks in the US healthcare sector. *International Journal of Research and Scientific Innovation (IJRSI)*, *10*(9), 177-193.

Olaniyi, O., Okunleye, O.J., & Olabanji, S.O. (2023). Advancing data-driven decision-making in smart cities through big data analytics: A comprehensive review of existing literature. *Current Journal of Applied Science and Technology*, *42*(25), 10-18.

Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction*, *60*, 102316.

Paiva, S., Ahad, M.A., Tripathi, G., Feroz, N., & Casalino, G. (2021). Enabling technologies for urban smart mobility: Recent trends, opportunities and challenges. *Sensors*, *21*(6), 2143.

Palleti, V.R., Adepu, S., Mishra, V.K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, *4*, 1-19.

Ramírez-Moreno, M.A., Keshtkar, S., Padilla-Reyes, D.A., Ramos-López, E., García-Martínez, M., Hernández-Luna, M.C., Mogro, A.E., Mahlknecht, J., Huertas, J.I., Peimbert-García, R.E., & Ramírez-Mendoza, R.A. (2021). Sensors for sustainable smart cities: A review. *Applied Sciences*, *11*(17), 8198.

Rani, S., Mishra, R.K., Usman, M., Kataria, A., Kumar, P., Bhambri, P., & Mishra, A.K. (2021). Amalgamation of advanced technologies for sustainable development of smart city environment: A review. *IEEE Access*, *9*, 150060-150087.

Rhee, S. (2020). 2019 Global city teams challenge: smart and secure cities and communities challenge expo. *NIST Special Publication*, *1900*, 204.

Rizi, M.H.P., & Seno, S.A.H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet of Things*, *20*, 100584.

Sanni, O., Adeleke, O., Ukoba, K., Ren, J., & Jen, T.C. (2024). Prediction of inhibition performance of agro-waste extract in simulated acidizing media via machine learning. *Fuel*, *356*, 129527.

Sarker, I.H. (2022). Ai-based modeling: Techniques, applications and research issues towards automation, intelligent and smart systems. *SN Computer Science*, *3*(2), 158.

Shandler, R., & Gomez, M.A. (2023). The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4), 359-374.

Soare, S.R., & Burton, J. (2020). Smart cities, cyber warfare and social disorder. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, 108.

Stellios, I., Mokos, K., & Kotzanikolaou, P. (2022). Assessing smart light enabled cyber-physical attack paths on urban infrastructures and services. *Connection Science*, *34*(1), 1401-1429.

Tan, S.Y., & Taeihagh, A. (2020). Smart city governance in developing countries: A systematic literature review. *Sustainability*, *12*(3), 899.

Turok, I., Seeliger, L., & Visagie, J. (2021). Restoring the core? Central city decline and transformation in the South. *Progress in Planning*, *144*, 100434.

Uyar, A., Nimer, K., Kuzey, C., Shahbaz, M., & Schneider, F. (2021). Can e-government initiatives alleviate tax evasion? The moderation effect of ICT. *Technological Forecasting and Social Change*, *166*, 120597.

Xia, L., Semirumi, D.T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, *98*, 104771.