Scientific Research Publishing

Journal of Information Security, 2024, 15, 134-147
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Artificial Intelligence Adoption for Cybersecurity in Africa

Nadine Nibigira[1], Vincent Havyarimana[2], Zhu Xiao[3]

[1]School of Engineering Sciences, University of Burundi Doctoral School, Bujumbura, Burundi
[2]Department of Applied Sciences, Burundi Higher Institute of Education (ENS), Bujumbura, Burundi
[3]College of Computer Science and Electronic Engineering, Hunan University, Yongzhou Hunan
Email: nibinadine@gmail.com, havincent12@gmail.com, zhu.xiao.work@gmail.com

How to cite this paper: Nibigira, N., Havyarimana, V. and Xiao, Z. (2024) Artificial Intelligence Adoption for Cybersecurity in Africa. *Journal of Information Security*, **15**, 134-147.
https://doi.org/10.4236/jis.2024.152009

Received: November 11, 2023
Accepted: March 18, 2024
Published: March 21, 2024

Abstract

Legacy-based threat detection systems have not been able to keep up with the exponential growth in scope, frequency, and effect of cybersecurity threats. Artificial intelligence is being used as a result to help with the issue. This paper's primary goal is to examine how African nations are utilizing artificial intelligence to defend their infrastructure against cyberattacks. Artificial intelligence (AI) systems will make decisions that impact Africa's future. The lack of technical expertise, the labor pool, financial resources, data limitations, uncertainty, lack of structured data, absence of government policies, ethics, user attitudes, insufficient investment in research and development, and the requirement for more adaptable and dynamic regulatory systems all pose obstacles to the adoption of AI technologies in Africa. The paper discusses how African countries are adopting artificial intelligence solutions for cybersecurity. And it shows the impact of AI to identify shadow data, monitor for abnormalities in data access and alert cyber security professionals about potential threats by anyone accessing the data or sensitive information saving valuable time in detecting and remediating issues in real-time. The study finds that 69.16% of African companies are implementing information security strategies and of these, 45% said they use technologies based on AI algorithms. This study finds that a large number of African businesses use tools that can track and analyze user behaviour in designated areas and spot anomalies, such as new users, strange IP addresses and login activity, changes to permissions on files, folders, and other resources, and the copying or erasure of massive amounts of data. Thus, we discover that just 18.18% of the target has no national cybersecurity strategy or policy. The study proposes using big data security analytics to integrate AI. Adopting it would be beneficial for all African nations, as it provides a range of cyberattack defense techniques.

Keywords

Artificial Intelligence (AI), Cybersecurity, Cyberattacks, Cybercriminals

1. Introduction

The increasing usage of the internet presents security teams with a number of obstacles, including sophisticated cyber-attackers, a growing attack surface, an explosion of data, and an increasingly complex infrastructure. These challenges impede their capacity to protect sensitive information, control user access, and promptly identify and address security threats. In Africa countries, AI systems are already deployed across many domains of daily life including housing, employment, transport, education, health, accessibility [1], and justice, and their use is likely to increase.

Recently, research firm Cybersecurity Ventures shared its "Top 10 Cybersecurity Predictions And Statistics For 2023," which unveiled the alarming fact that global cybercrime financial damage will reach $8 trillion in 2023 and $10.5 trillion by 2025. In 2018, there were a handful of countries namely Kenya, South Africa, Nigeria, Ghana and Ethiopia [2] where AI had already been applied

Of course, cybercriminals often use AI for their own purposes, including creating new malware and hacking tools, automating phishing attacks, searching for loopholes in security, and using deep fake technology and malicious bots to impersonate people. But at the same time, AI enables us to fight back better than ever before.

Artificial Intelligence (AI) is increasingly being incorporated into business processes and systems [3]. But not all industries are equally sophisticated: IT and telecommunications are the most advanced sector for adopting AI, while cars lag behind these numbers. There are already numerous applications of AI in Africa, particularly in the areas of health, water supply, clean energy forecasting, climate change prediction, economics and finance, and governance [4].

During a lecture hosted by United Nations University Institute for Natural Resources in Africa (UNU-INRA), Nature Speaks: Artificial Intelligence and Growth, at the University of Ghana on 25 May 2023, Professor Tshilidzi Marwala, Rector of the UNU and former Vice-Chancellor of the University of Johannesburg, shared insights on how Artificial Intelligence can contribute to the achievement of the sustainable development goals in Africa. Professor Alexander Adam Kwapong Lecture on Artificial Intelligence and Economic Growth, examined the relationship between AI and economic growth in Africa, exploring this exciting technology's unique challenges and opportunities. The crucial factors needed for technology adoption are sadly lacking across most of Africa, and many countries in Africa are still lacking the necessary infrastructure, governance, data ecosystem, STEM education, and other factors necessary for AI [5]. We will discuss how AI is already being used to drive growth in various African

countries, from improving healthcare outcomes to enhancing agriculture and financial services.

AI will be becoming more essential to handle cyber-threats in the area of cybersecurity: fact, the market is projected to expand [6]. At the same time, the use of AI is not without dangers: over 60 percent of AI businesses recognize that AI creates the most significant cybersecurity concerns [7]. AI, being a general-purpose, dual-purpose technology, has the potential to be both a boon and a bane for cybersecurity.

The fact that AI is employed as a sword [8]. With an added twist: because the use of AI for national security purposes experiences many limitations, particularly as government agencies keep moving to monitor and control high-risk applications and encourage greater AI use, on the attack side, the most malicious applications keep increasing, the cost of new applications falls, and the 'threat landscape' becomes denser with each passing day.

The AI technology also helps identify vulnerabilities and defend against cybercriminals and cybercrime. It compares the anomalies, It uses its knowledge base to identify and predict the possible next steps and likely outcomes of the unusual events. Once AI identifies a potential threat, it can take prescribed actions such as preventing deletions, logging off suspicious users and notifying operators of the suspected malicious activity [3]. By automating incident responses using AI-driven tools we can respond to security incidents in real-time. This includes isolating affected systems, blocking malicious traffic, and implementing predefined response strategies.

Automated responses will institutions mitigate the impact of cyberattacks and reduce the time between detection and response. African Countries can then review the findings and take further action if needed. And African Governments should prioritize building and expanding digital infrastructure to reach underserved areas, including rural and remote communities. Indeed, a lot of African nations still lack comprehensive information security laws, which makes it challenging to combat cyber threats and complicates the adoption and enforcement of cybersecurity measures. Just 39 of the 54 African countries have passed cybersecurity laws to date, and two more are still working on their drafts. The adoption rate of cybersecurity laws and regulations on the continent as a whole is 72%, which is the lowest rate globally. The African Union Convention on Cyber Security and Personal Data Protection has only been approved by 14 nations.

2. Artificial Intelligence in Cybersecurity

Cybersecurity is a rapidly developing subject that has been in the news often over the past decade, as the number of risks continues to grow and cybercriminals strive to remain one step ahead of law.

Defining African AI:

1) Generated with machine learning and deep learning algorithms

2) Created by AI developers located in Africa

3) Created by companies composed primarily on African developers creating AI specifically for in Africa

4) Operational at the time of data collection

5) Created by companies that were operational at the time of data collection

Artificial Intelligence (AI) presents enormous global opportunities: it has the potential to transform and enhance human well-being, peace and prosperity. To realise this, the author affirms that, for the good of all, AI should be designed, developed, deployed, and used, in a manner that is safe, in such a way as to be human-centric, trustworthy and responsible.

The African Union (AU) established the Working Group on AI in 2019 with the intention of developing an African position on AI technologies. The "African Union Artificial Intelligence (AU-AI) Continental Strategy for Africa" was drafted in 2023 by the African Union Development Agency (AUDA-NEPAD) and the AU High-Level Panel on Emerging Technologies (APET). It is anticipated that a version that has been adopted continentally would be presented in January 2024 at the African Union Summit of Heads of State and Government.

2.1. Dataset

2.1.1. Data Sampling

The target country of the sample study country following the below formula:

$$\text{Sample target} = \frac{n}{n_1} = \frac{56}{5} = 11 \quad (1)$$

where n = all African countries = 56 and n_1 = African Region = 5

The paper considers the 56 African countries from 5 regions, the following table shows the eleven target countries.

Table 1. Target countries with their region.

Region		Country
Southern Africa	1	Lesotho
	2	Botswana
South Africa Middle Africa	3	Cameroon
Eastern Africa	4	Burundi
	5	Kenya
	6	Rwanda
	7	Uganda
Western Africa	8	Ghana
	9	Nigeria
Northern Africa	10	Algeria
	11	Morocco

2.1.2. Data Collection

Data was collected from eleven targets countries of African from 154 companies, ONGS and start-ups which characterize by Enterprise (E) in data set due to the data confidentiality.

2.2. Mapping Artificial Intelligence in AFRICA

Many studies on Higher education observed that the academic performance is influenced by the academic infranstrures and financial resources. Many governments, and universities in Africa support AI projects. However, most of African's budget is insufficient, hindering the delivery of high-quality AI applications. African government, companies, ONG many higher educations, ministries engaged in embracing AI/technology to achieve socio-economic development.

As the world continues to embrace the use of AI in various sectors, Several African countries are not left behind. African countries are countries showing a keen interest in adopting AI to improve service delivery, increase efficiency, fraud detection, etc, and boost their economic growth. However, the adoption of AI in Africa countries met several challenges.

Several reports on States' adoption of Artificial Intelligence AI across the world have indicated that African countries have a "slow" or "low" AI adoption rate. This position is, however, changing, as several African countries are now bringing a modest acceptance of AI into different aspects of their governance structures and institutions. With what this study characterizes as an era of "AI normative emergence in Africa", here are seven ways that this technology is being legitimized and integrated by African states today:

- Developing National AI Strategies
- Establishing AI Agencies, Task Forces and Commissions
- Amending Existing Laws and Creating New Regulations
- Building Strategic Partnerships
- Initiating Public Sector Reform with AI
- Driving AI Education, Training and Research
- Fostering A Continental (African) Approach to AI

The following **Table 2**, summarize how the eleven countries are adopting AI

Africa's susceptibility to cyberattacks is rising along with the continent's adoption of digital transformation initiatives. The most common cybercrime risks seen in Africa, according to Interpol, are ransomware, botnets, digital extortion, business email compromise, and online frauds. Studies conducted by the cybersecurity firm Serianu, situated in Kenya, show that the expense of cybercrime in Africa has grown from US$0.5 billion in 2015 to US$3 billion in 2020. A total of 39 African nations Côte d'Ivoire, Egypt, Ghana, Kenya, Morocco, Nigeria, Rwanda, Senegal, and South Africa have passed legislation specifically addressing cybercrime. These laws usually include provisions pertaining to international collaboration in combating cybercrime. Legislation pertaining to data protection and electronic transactions occasionally refers to cybercrime, as is the case in Ghana.

Table 2. AI adoption in Africa countries (data collect on Openai Africa [7]).

Country	Areas of application	Policy Priority
Rwanda	Driving AI-Specific Education, Training and Research Initiating Public Sector Reform with AI Building Strategic Partnerships	Google's support with graduate programs in Machine Intelligence at the African Institute for Mathematical Sciences center in Rwanda. Rwanda has enlisted anti-epidemic robots in its fight against the coronavirus Rwanda's 10-year contract with Babyl (a digital healthcare provider), to create Africa's first universal primary healthcare service, which introduces an AI-powered triage and symptom-checker platform; drone delivery service with Zipline, which delivers medicine and blood to otherwise difficult-to-reach areas; and partnership with the World Economic Forum to increase the country's diagnostic capacities for detecting cancer.
Lesotho	Driving AI-Specific Education, Training and Research	In Lesotho, the Department of Mathematics and Computer Science in the National University of Lesotho is now mandated to include research on AI systems and projects.
Bostwana	Developing National AI Strategies	Botswana's plan to use AI through its Science, Tech and Innovation Action Plan to foster economic growth and job creation was approved by the President's Cabinet in September 2019 and scheduled for submission to Parliament for adoption.
Cameroon	Driving AI-Specific Education, Training and Research	Cameroon opened its first AI Centre at the University of Yaounde. Hosted at the National Advanced School of Engineering, Polytech, of the University of Yaounde, the Centre provides top-notch services for students, trainers, companies as well as other partner organisations.
Uganda	Establishing AI Agencies, Task Forces and Commissions Promulgating AI Laws and Regulations Initiating Public Sector Reform with AI Building Strategic Partnerships	Uganda's national AI taskforce will focus on addressing local issues, including increasing agricultural production, on which the largest percentage of the country's population relies. Uganda set up its taskforce to advise government on domesticating AI to fast-track the country's economic development. expressed a desire to negotiate a new international instrument. The aim of the treaty is to address concerns over lethal autonomous weapons. Uganda, it is also used to detect gunshots in South Africa.
Burundi	Driving AI-Specific Education, Training and Research	Researches are interesting on AI and Cybersecurity
Kenya	Establishing AI Agencies, Task Forces and Commissions Initiating Public Sector Reform with AI Building Strategic Partnerships	Kenya established a Blockchain & Artificial Intelligence Taskforce to contextualize the application of AI in areas of the country's financial inclusion, cyber-security, land titling, election and single digital identity processes. Blockchain technology is being used by government departments in Kenya, including the respective Ministries of Lands and Health The African Development Bank's partnership with Microsoft to launch the Coding for Employment Programme in Côte d'Ivoire, Kenya, Nigeria, Rwanda, and Senegal.
Ghana	Promulgating AI Laws and Regulations Building Strategic Partnerships	At the United Nations (UN), Ghana, supported by Sierra Leone, South Africa, Uganda, Zambia, and Zimbabwe, amongst other non-African States, expressed a desire to negotiate a new international instrument. The aim of the treaty is to address concerns over lethal autonomous weapons. Google's first Africa AI lab in Ghana, providing developers with necessary research to build products that can solve Africa's unique problems.

Continued

Nigeria	Establishing AI Agencies, Task Forces and Commissions Promulgating AI Laws and Regulations Building Strategic Partnerships	Nigeria has announced the establishment of its National Agency for Research in Robotics and AI, which will leverage collaborations with international research bodies on robotics and AI and enable AI education for the country. Kenya's new data protection law complies with European Union legal standards, placing restrictions on how personal data can be handled, stored and shared. The same applies to South Africa's Protection of Personal Information Act and Nigeria's Data Protection Regulation of 2019. In the three cases, applicability to AI can be inferred where personal data is involved in AI-based transactions.
Egypt	Developing National AI Strategies	Egypt has set their AI strategy on two main axes, namely a specialized AI academy, and [6] using AI for governance and business enterprises driven by data science.
Morocco	Driving AI-Specific Education, Training and Research	In Morocco, the UEMF is opening its doors to the Euromed School of EIDIA, a brand-new center dedicated towards AI research, development, and education. Also, Morocco's AI training programmes supported by the French Ecole Polytechnique.

AI technologies are an opportunity for Africa to accelerate productivity and reimagine its economic growth, which is, more than ever, vital for the welfare of the world. This table helps with data analysis as it provides information on the use of AI in the eleven-country target. It is visible that AI in Africa countries contributes to economic development, which also goes hand with the protection of infrastructures.

This shows that the nature of AI holds promise for bringing about fundamental socio-cultural changes in Africa, including in areas such as political activities, poverty alleviation, environmental sustainability, transportation, agriculture, healthcare, education, financial transactions, and religious and traditional belief systems. Many of these AI systems are no longer described as dreams but are becoming a reality in Africa, though mainly driven by companies with roots in the Global North.

The big technology companies establishing operations in Africa, home-grown experts are increasingly establishing technology spaces similar to the US Silicon Valley and Silicon Wadi in Israel. These tech spaces and many African networks, local AI start-ups, and local stakeholders are fostering a growing ecosystem aimed at developing AI systems that are sensitive to African interests, concerns, and culture.

2.3. Limitations of Applying AI in AFRICA

A large number of nations have implemented national cybersecurity policies and plans, creating organizations to tackle cybercrime, defining goals and objectives, and delineating aspects of global collaboration on cybersecurity matters. 39 African countries have laws that specifically addressed cybercrime in 2021, according to the United Nations Conference on Trade and Development. Several

SADC countries, including Zimbabwe, Zambia, Botswana, Tanzania, Malawi, and Tanzania, have included cybersecurity legislation.

The first difficulty is epistemic: how AI security risk may be comprehended in a sufficiently broad yet coherent frame. Only then can the ability of African nations to respond to AI security risk be properly appraised. It is necessary to investigate whether risk management and cybersecurity systems already in place adequately understand and characterize the risks related to artificial intelligence. If hazards are not acknowledged in a comprehensive framework, gaps will occur and reactions will continue to be disjointed. A piecemeal approach may cause some dangers to go unnoticed or worsen, while adequately addressing others. For policymakers to understand the problem and the need for a solution, the importance of AI security risk must to be brought to light.

Despite its vast potential, the adoption and implementation of AI in Africa face several challenges, including a lack of relevant technical skills, Labor pool, Financial resources, data limitation, inadequate basic and digital infrastructure, uncertainty, lack of structured data, lack of government policies, ethics, user attitudes, insufficient investment in research and development, and a need for more flexible and dynamic regulatory systems.

Although artificial intelligence (AI) has promise for quickening Africa's economic transition, there are also worries about the risks involved. One of the main obstacles to AI adoption in Africa is the lack of appropriate technical skills, especially among youth. To support this, practitioners and researchers need to be familiar with statest cybersecurity measures. Numerous experts in artificial intelligence have voiced their worries that the development of AI and other technologies may have a number of unexpected economic repercussions. These worries, in general, include commercial and job disruptions as well as the exacerbation of already-existing structural disparities.

In particular, the use of artificial intelligence to combat cybercrime.

The digital infrastructure revolution is well underway, across the world and there are fears that Africa will behind as the digital divide grows. The achievement of AI applications depends on the availability of high-quality and diverse data. In Africa, there is a significant challenge in ensuring that AI systems are trained on data that accurately reflects the local population and addresses the unique challenges faced by the continent.

3. Results, Findings and Discussion

During this research, respondents confirmed that the goals of developing an information security strategy help them to clearly define and develop metrics to determine the goals and follow up on those goals are being achieved. The fully meshed and collaborative approach of a security fabric is the ideal way to enable secure business growth and effective risk management, especially when IT budgets and resources are constrained.

According to the survey findings, majority of respondents have a general understanding of what intelligence security, Artificial Intelligence and cybersecurity are. 45% indicated that they are using technologies which are built with AI algorithms to fight against cyberattacks. Table 2 shows how Africa is using artificial intelligence to achieve collaborative success and overcome outstanding challenges and bottlenecks

The study found that only 18.18% of the targets don't have national cybersecurity policies and strategies.

The national cybersecurity policies of Nigeria and Rwanda, as well as the cybersecurity law of Kenya, emphasize international collaboration in handling cybercrime concerns (e.g., in detecting and deterring cyberespionage and responding to cybercrime). Nigeria's Cybercrime Act has a whole section devoted to foreign cooperation in law enforcement and jurisdictional matters.

The creation of a National Cyber Security Agency is outlined in Rwanda's National Cybersecurity Strategic Plan. The agency supports research and development in the field of cybersecurity as well as regional and global cooperation. Membership in regional and global CERTs, international collaboration in the fight against cybercrime, and international information exchange are further strategic initiatives pertaining to international cooperation.

On August 5, 2022, the Kenyan government unveiled their national cybersecurity plan, which serves as a road map for addressing new issues and rising threats in the cyberspace.

Law No. ˚1/10 of March 16, 2022 on the prevention and repression of cybercrime in Burundi was put into effect with the intention of stopping and suppressing all cyber offenses committed both inside and outside of the country, as well as all criminal offenses whose detection necessitates the gathering of electronic evidence. The Government of Burundi continues to initiate and promote numerous cybersecurity policy and legal initiatives.

International collaboration in cybersecurity and AI research and training is also mentioned in a number of policy documents. Rwanda's cybersecurity policy mentions participating in international research projects and exchanging cybersecurity experts, whereas the Nigerian Cybercrime law emphasizes the need to organize training and capacity development programs for officials responsible for the prohibition, prevention, detection, investigation, and prosecution of cybercrimes. Additionally, Senegal's policy encourages courts and law enforcement organizations to work together with partners on a bilateral and global scale to enhance their efforts in locating, preventing, and prosecuting cybercrime.

3.1. Sensibilization on the Adoption of AI

Everything starts with culture, there needs to be a strong cultural shift. Artificial Intelligence (AI) techniques are being utilized more often in higher education to improve both student and instructor learning. An extensive analysis of artificial

intelligence of this study in higher education from 2016 to 2023 found that the technology has been applied to controlling student learning, assessment and evaluation, prediction, AI assistants, and intelligent tutoring systems in Africa.

All respondents (100%) confirm that they have started the awareness about AI and cybersecurity. However, it is noted that there is a low levels of awareness in the Africa countries, so it is not surprising t when it comes to reporting cybercrime to the police

African countries through different regions are actively engaging in threat sharing in order to avert possible crime, ensure heightened awareness and security compliance amongst network providers; and publicly expose and appropriately sanction cyber criminals when caught to serve as a deterrent to the public. This study discover that the National Central Bureau of Interpol also is helping to against cybercrime in different region in Africa.

3.2. The Adoption of AI Technology to against Cyberattacks

African Governments in their different projects, are prioritizing, building and expanding digital infrastructure to reach underserved areas, including rural and remote communities. Ensuring that all students have access to a reliable internet connection and appropriate devices, which may involve government and public-private partnerships. Africa Countries work towards reducing the cost of internet access and technology devices. This is achieved through government grants, community programs, or educational institution initiatives to provide affordable or loaned devices to students in need. African Industries are majorly fed by global knowledge base, the whole open knowledge, open data and open science paradigm.

Figure 1 shows the level of adoption of AI technologies in Africa

It's important that, in Africa, 45% of targets already AI technologies take the place of traditional teaching techniques or human teachers. AI tools ought to be utilized to improve and augment the educational process instead.

By automating incident responses using AI-driven tools we can respond to security incidents in real-time. This includes isolating affected systems, blocking malicious traffic, and implementing predefined response strategies. Automated

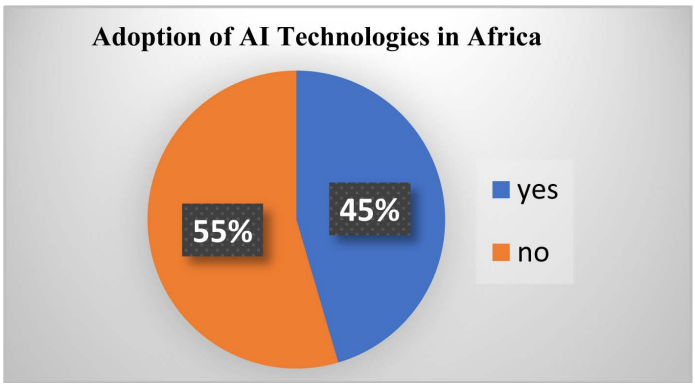

Figure 1. AI Technologies adoption.

responses will institutions mitigate the impact of cyberattacks and reduce the time between detection and response.

3.3. Policy Frameworks are in Place to Inform the Adoption and Use of AI

This study found that 86.3% of targets, have in their system firewall and endpoints tools with an extra layer of security; to defeat the latest and most dangerous malware and provide real-time protection on the company's desktops and mobile devices. Those tools are built with AI and offer fully managed and layered security measures.

Vulnerability analysis for critical infrastructures involves identifying weaknesses and potential risks within systems that support essential services such as power grids, transportation networks, communication systems, and water supplies. This analysis helps identify potential vulnerabilities and assess the potential impact of threats, enabling organizations to develop strategies for mitigating risks and enhancing the security of these infrastructures.

3.4. Discussion

People all around the world are already greatly impacted by AI technologies, and this trend is only going to get stronger in the near future. And with artificial intelligence "spreading" throughout the continent, Africa is not an exception to this tendency.

This study concludes that information security measures are being used by 69.16% of the dataset used, which comes from eleven target countries. The paper states that although safety needs to be considered in all African nations, actors who are developing frontier AI capabilities that is, AI systems that are exceptionally powerful and potentially harmful have a special responsibility to ensure the safety of these systems. This responsibility includes developing systems for safety testing, conducting evaluations, and taking other necessary steps. In order to minimize misuse, control concerns, and the exacerbation of other risks, it is imperative that all pertinent actors offer context-appropriate transparency and responsibility regarding their intentions to assess, monitor, and mitigate potentially harmful capabilities and any associated repercussions that may arise.

After analysing the situation in Africa, the research proposes the adoption in all Africa countries of Big Data Security Analytics tools, algorithms and techniques in order to protect critical information infrastructures against cyberattacks. Big Data Security Analytics is an advanced method for protecting sensitive data and digital assets. It makes use of supervised learning techniques, artificial intelligence (AI), and machine learning.

It provides organizations with a proactive and data-driven approach to protect critical information infrastructures against cyber-attacks. Analytical methods including data mining, machine learning, artificial intelligence, statistics, and natural language processing are used in big data security analytics. With the

support of artificial intelligence and machine learning, the solutions provide promise that systems and companies may be kept safe from cyberattacks and breaches.

3.5. Business Impact Analysis

AI is creating African Solutions to African Problems in all domains. It is helping African countries the main abilities to combat cybercrime in real-time through the AI technologies. Africa is integrating AI across various sectors of its economy. With a strong emphasis on responsible and ethical use, the policy aims to position Rwanda as a global leader in AI innovation while fostering sustainable economic growth and social development.

4. Future Works and Conclusion

Although there are many prospects for sustainable growth associated with the extensive use of AI in Africa, there are also significant hazards associated with it in a number of areas, including cybersecurity. Consequently, collaboration on cybersecurity among all stakeholders—including governments, corporations, academics, non-governmental organizations, and others becomes more crucial. In order to ensure a future cyber safe for the African continent, Kaspersky, for its part, adamantly supports every effort already made in this area and declares its readiness to continue contributing to current and future projects in this field.

AI adoption in Africa raises ethical questions that need to be resolved in order to make sure the technology is applied for the benefit of society as a whole. When using AI, ethical factors including bias, job displacement, responsibility, transparency, security, and privacy need to be considered. Involving all relevant parties in the conversation on ethical issues surrounding the deployment of AI is crucial. These parties include the government, business, civil society, and academic institutions.

This will make it possible to guarantee that AI is applied to better rather than worsen people's lives. Concerns over risk management and data privacy for individuals and enterprises are only going to increase as AI develops. Regulators are thinking about how to advance AI and optimize its positive effects while lowering the possibility of detrimental effects on society. However, the African States do not yet have any comprehensive federal regulation pertaining to AI, and everyone involved must contribute to guaranteeing the security of AI. The study concludes that African countries need to adopt analytical methods including data mining, machine learning, artificial intelligence, statistics, and natural language processing which are used in big data security analytics. With the support of artificial intelligence and machine learning, big data analytics solutions provide promise that systems and companies may be kept safe from cyberattacks and breaches and all Africa will be safe.

In the future, we hope to build AI models and algorithms that will support African nations in their fight against cyberattacks, particularly in the areas of

malware filtering, fraud detection, and mobile transactions.

Declarations

Availability of Data and Materials

Data Materials

The entire dataset is available in a spreadsheet format and was collected through different online platforms and interviews. For this work, a questionnaire was create that helped to collect information. The data sharing agreement was signed and approved by the author and responder during data collection phase.

Code Availability

No specific code was generated for analysis of these data.

Funding

This work was supported by the authors of this work

Author's Contributions

Nadine NIBIGIRA Conceptualization, Visualization, Methodology, Investigation, Writing Original Draft and Fund the paper. Pr Vincent HAVYARIMANA Supervision, Validation, data analysis, resources. Pr Zhu Xiao Formal analysis, data curation, Editing the paper.

Acknowledgements

First of all, we would like to thank Almighty God for giving us strength, peace of mind and good health. This study is the result of the symbiotic framework where inspiration found in many directions. We would like to thank everyone from far or near who has contributed, directly or indirectly, to this work. we believe it could not have found better ingredients for it. We hope the results will serve for all African countries and researchers who will be working on similar topics. The authors in this paper acknowledge also all other authors whose work was used as references in this paper.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Salloum, S.A., Alshurideh, M., Elnagar, A. and Shaalan, K. (2020) Machine Learning and Deep Learning Techniques for Cybersecurity: A Review. *Advances in Intelligent Systems and Computing*, 50-57. https://doi.org/10.1007/978-3-030-44289-7_5

[2] Atlantic Council Africa Center (2018) Coming to Life: Artificial Intelligence in Af-

rica Issue Brief November 2018 Aleksandra Gadzala.

[3] Anyoha, R. (2017) The History of Artificial Intelligence. Science in the News-Harvard University, 1-19.

[4] Dumitras, T. and Shou, D. (2011) Toward a Standard Benchmark for Computer Security Research: The Worldwide Intelligence Network Environment (WINE). *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, Salzburg, 10 April 2011, 89-96. https://doi.org/10.1145/1978672.1978683

[5] Ade-Ibijola, A. and Okonkwo, C. (2023) Artificial Intelligence in Africa: Emerging Challenges. In: Eke, D.O., Wakunuma, K. and Akintoye, S., Eds., *Responsible AI in Africa*, *Social and Cultural Studies of Robots and AI*, Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08215-3_5

[6] National Academies of Sciences (NAS) (2020) Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. National Academies Press.

[7] Seven Ways that African States are Legitimizing Artificial Intelligence. https://openair.africa/7-ways-that-african-states-are-legitimizing-artificial-intelligence/

[8] AI Is Here to Stay! How Artificial Intelligence Can Contribute to Economic Growth in Africa. https://reliefweb.int/report/world/ai-here-stay-how-artificial-intelligence-can-contribute-economic-growth-africa#:~:text=There%20are%20already%20a%20number,finance%2C%20as%20well%20as%20governance

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
UNU-INRA	United Nations University Institute for Natural Resources in Africa
EIDIA	Euromed School of Digital Engineering and Artificial Intelligence
UN	United Nations
UEMF	Euromed University of Fez