International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Contemporary Cybersecurity and Privacy Challenges in Africa's Evolving Digital Landscape

A Systematic Analysis of Threat Trends and Data Protection Frameworks

Vansh More
Department of Computer Science
Dr.DY Patil Arts Commerce Science College
Pimpri,411018
Pune, India

Amit Pawar
Department of Computer Science
Dr.DY Patil Arts Commerce Science College
Pimpri,411018
Pune, India

ABSTRACT

The rapidly evolving digital landscape in Africa was significantly contributed to economic growth and enhanced social connectivity through widespread adoption of mobile, digital banking, cloud computing, and daily life use of AI and ML. The digital transformation has also expanded the cyberattack surface across the continent, as a result challenges are increased in cybersecurity and privacy. Recent studies show a sharp increase in cyber incident targeting African organizations, mainly targeting the weak cybersecurity policies, limited digital educations, and low knowledge about cyber threats like RANSOMWARE. This research paper about the current cybersecurity and privacy challenges in Africa's analyzing cyber incidents from different area, including north, east, west and south Africa including cyberattacks in 11 African countries . The study highlights major issue like data branches, identity theft, Not proper or complete legal and regulatory frameworks, shortage of skilled cybersecurity professionals, and poor security in important sectors like financial services, education sectors, media and telecommunication. The research paper discusses the duel role of AI and ML, which no new hand create risks, but on the other hand help in threat detection and response. This paper increasing public knowledge about data protection for better education and investment in secure digital infrastructure. It also points out the importance of regional and international cooperation, data sharing, and public privet partnership. The study concludes the inclusive and collaborative approach is Mandatory to insure secure digital growth and effective privacy protection in Africa's developing digital ecosystem.

Keywords : Cybersecurity, Privacy Protection, Digital Transformation, Africa, Cyber Attacks, Ransomware, Data Breaches, Identity Theft, AI and Machine Learning, Digital Banking, Mobile Technology, Legal and Regulatory Frameworks, Cybersecurity Skills Gap, Critical Infrastructure security.

I. INTRODUCTION

Africa's Digital Landscape Has Fastly Transformed In The Last 15 Years, Because Of The Adaptation Of Mobile Technologies, Digital Banking Platforms, Cloud Computing Solutions, And Emerging Technologies Such As Artificial Intelligence And Machine Learning. These Digital Innovations Have Enabled Broader Economic Participation, Improved Access To Government And Financial Services, And Reduced Communication Among Individuals, Businesses And Institutions All Over The Continent. The Growth Of Mobile Money And Digital Payment Systems, Ṣfor Example, Has Clearly Boosted Financial Inclusion By Allowing Millions Of Citizens Outside The Formal Banking System In The Formal Economy.

Countries Across The Landmass Are Integrating AI Powered System Into Critical Operations Such As Scam Identifications, Customer Services Automations, And Data Based Forecasting, Reflecting A Growing Reliance On Digital Resources As Foundational Elements Of Modern Economical Infrastructure. One Of The Biggest Challenge In African Countries Face Is Building A Strong And Effective Legal Framework For Cybersecurity And Data Protection. The African Union Convention On Cybersecurity And Personal Data Protection, Commonly Known As The Malaba Convention, Was Introduce To Harmonize Cybercrime Laws Across Member States. However, Its Implementation Has Been Consistent, Leading To In Gaps Enforcement And Across Border Corporations. Weak Regulatory System Reduce The Ability Of Government And Public Sector Or Organizations To Respond Quickly To Cyber Threats And Ensure That Offender Are Accountable.

Another Major Concern Is Shortage Of Skilled Cybersecurity Professionals Across The Countries. This Skill Gap Makes It Difficult For Organizations To Properly Design, Manage And Protect Secure Digital Systems. It Also Limits National Efforts To Implement Comprehensive Cybersecurity Strategies.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

In Africa, Many People Rely Heavily On Their Phones For Money And Business Transactions. This Is Benefits As As It Provides Access To Banking Services For These Who Providely Had None. However, It Also Creates Opportunities For Theft. Criminals Can Steal Phone Numbers, Infect Devices With Viruses, Or Capture Login Information. Therefore, It Is Crucial To Ensure Our Mobile Phones Are Secure Against These Attaks. With The Growth Of Banking And Mobile Money Services, We Just Prioritize Security On Our Phones To Prevent Theft.

Cybercriminals Have Also Begun Using Intelligence Tools, Allowing Them To Conduct More Complex Attacks. These Attacks Involve Automated Phishing And The Creation Of Realistic Deepfake Content, Making It Even More Challenging To Detect And Stop Threats From These Criminals. Many Of These Attacks Employ Artificial Intelligence Tools.

Despite These Risks, Artificial Intelligence And Machine Learning Present Promising Solutions For Improving Cybersecurity. When Used Responsibly, These Technologies Can Enhance Threat Detection, Identify Different Behavior In Real Time, Automate Incident Responses, And Analyze Big Datasets To Predict Emerging Attack Patterns. Research Into AI-Based Cybersecurity Frameworks In Africa's Resource-Limited Environments Shows That Properly Governed AI Systems Can Outperform Traditional Rule-Based Defense Methods While Maintaining Accountability And Flexibility.

Despite Rapid Digital Expansion Across Africa,Cybersecurity Readiness Has Not Progressed At The Same Speed. The Mismatch Between Digital Development And Cybersecurity Capacity Has Exposed The Financial Sector To Greater Risks And The Government Institutions, And Smartphone Platforms. Increasing Reliance On Digital Technologies Without Sufficient Security And They Endanger Both Financial Stability And Individual Information Privacy .

To Overcome The Cybersecurity And Information Privacy In Africa , We Need To Show More Efforts And Diverse Strategies Are Essential. We Have Make The Rules More Stronger Because People Should Know About Spend Money On Safe Digital Websites , Improved The Knowledge About Cybersecurity And Tell Individuals About The Harm Of Cyber Attacks. This Is Very Important To Keep Our Individuals Safe . We Also Need To Explore Our Work In Other United Countries And Regions To Explore More Informations ,Reacts To Problems Together And Ensure Our Policies Remains Aligned.

Cyber Security Is A Critical Key Consideration And We Must Implement These To Enhance Our Protection. We Need To Prioritise Cybersecurity. Such Cooperation Can Help To Assure That African Countries Not Merely Adopt Technologies But Also Adopt A Cultivated Resilient Digital Ecosystem Able To Mitigate Evolving Cyber Threats.

This Study Is Designed To Analyze The Territorial Distribution Of Cyber Incidents Throughout Africa, Identify Major Types Of Cyber Attacks, Study Sector-Wise Weaknesses, Determine The Cybersecurity Skill Gap, And Evaluate The Dual Role Of Artificial Intelligence And Machine Learning In Strengthening Digital Security.

II. LITERATURE REVIEW

The fastest digital transformations happening over Africa is getting attention from people who study about policymakers and international organizations.Certain studies show that many people are using thechnologys like digital banking, cloud and internet based services. Some studies show that many people are using technologies like digital banking, cloud computing, and internet-based services. This has helped the economy grow and allowed the government to function better. It has also made it easier for people to connect with one another. The World Bank states that mobile money and digital financial services have helped bring people into the banking system. They now have access to banking services that were previously unavailable, especially for those who could not use banks at all.

The digital transformation across Africa is changing the landscape. Mobile money and digital financial services play a key role in this change, ensuring that more people have access to banking services. Experts believe that the internet and digital platforms have enabled new businesses to emerge, allowed companies to deliver services easily, and fostered new ideas in various fields across Africa. Digital platforms have significantly impacted Africa. They have supported the launch of new businesses and simplified the delivery of services. These platforms have also encouraged innovative ideas.

Africa is Undergoing rapid growth in digital technology. However, this swift digital advancement also Offers Expanded cybersecurity and privacy risks. The International Telecommunication Union and other cybersecurity organizations demonstrate that African countries are Facing multiple cyber incidents, including ransomware attacks, phishing attempts, data breaches, and identity theft. Therefore, systems are now vulnerable to cyber attacks. Cybersecurity is a concern in Africa due to this gap. The continent needs to focus on developing its cybersecurity frameworks to prevent attacks. The difference between rapid digital growth and security readiness is identified as a major challenge in the literature.

Researchers are examining cybersecurity risks specific to various sectors in Africa. In sectors like services and digital banking, cybercriminals are especially active. These sectors conduct many transactions online and must keep customer information safe. Studies on government institutions and public sector organizations show that they face challenges due to inadequate funding for cybersecurity and lack of preparedness for incidents. Cybersecurity risks show major concern in these sectors. Researchers aim to examine how

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

these risks affect different industries, as well as financial services, digital banking, government institutions, and public organizations. In education, healthcare, media, and telecommunications, security measures are not sufficiently established. This deficiency makes these sectors attractive targets for cyber threats. Workers in education, healthcare, and media often lack sufficient knowledge about computer security, which increases Security weakness.

Regulatory challenges continue to be key issues in discussions about cybersecurity and data protection in Africa. While many countries have put legal frameworks in place, implementation is often irregular. The African Union launched the Malabo Convention to align cybersecurity and data protection laws on a continental scale. However, slow ratification and uneven implementation have limited its impact, leading to fragmented regional integration efforts.

Cross-border cybercrime compounds the difficulties of enforcement. Cyber threats often arise from external sources along national borders, making it hard to investigate and prosecute due to differing laws and limited technical skills. International cooperation Is fundamental but remains problematic. A major issue is the lack of skilled cybersecurity professionals. The skills gap between present capacity and necessary expertise results from limited access to specialized education, training, and certification programs. This shortage weakens the readiness of institutions and their ability to respond incidents. Additionally, low public awareness and limited digital skills increase vulnerability to phishing and social engineering attacks, Pointing to the significance of awareness initiatives.

Artificial Intelligence and Machine Learning are taking on expanded roles in shaping cybersecurity strategies. While attackers may use these technologies to create advanced threats, they also play a role in improving defense efforts by allowing real-time threat detection and automated analysis. This is especially useful in environments with limited resources.

Research indicates a disparity between rapid digital growth and inadequate cybersecurity funding. Countries with stronger enforcement and organized national strategies experience fewer critical disruptions. As a result, improving regulatory implementation, workforce training, public awareness, and regional cooperation is crucial.Cybersecurity and privacy in Africa interconnected issues that need a coordinated and inclusive approach. This study adds to the existing literature providing a regional analysis of cyber incidents and looking at the evolving role of AI and ML in boosting digital resilience.

III. RESEARCH METHODOLOGY

This research adopts a qualitative approach to examine current cybersecurity and privacy challenges in africa's changing digital environment. The study aims the understand the nature of cyber threats, existing vulnerabilities, and factors that contribute to cyber security risk across different regions. A qualitative strategy is appropriate since it enables detailed examination of existing studies, reports, and recorded cyber incidents rather than emphasizing only numerical data.
The research design descriptive and exploratory. Its system describes current cybersecurity conditions while exploring patterns throughout regions and sectors. The study not collecting primary data, it reies completely on secondary documented evidence. We focus on information that is already gathered from trustworthy source. These include peer reviewed journals, conference papers, government publications,report from organisastions like the African union, and cybersecurity companies. We need Google schooler to find information on keeping our data safe online, the shift to digital platform, and the use of artificial intelligence and machine learning in cybersecurity. We specifically looked for relevant information on AI and ML they relate our topic. We choose only recent publications to ensure accuracy.

The study examines incidents throughout various parts of Africa, including North, East, West, and South Africa. It examines cyberattacks from several countries to identify common threats. They also include ransomware, identity theft, social engineering, and online scams. The study focuses on significant areas like banking, government offices, schools, media outlets, telecommunications, and online banking services. Cyber incidents and attacks are a critical issue, and the research aims to understand their effort on Africa. By studying these incidents, we can gain more insight into how cyberattacks operate. These sectors were selected based on their growing reliance on digital technologies and importances for economic and social stability.

A comparative and thematic analysis method is used to assess the data collected. Cyber incidents and research findings are compared across regions to identify similarities, differences, and recurring patterns in cybersecurity challenges. Key themes such as weak cybersecurity policies, insufficient legal and regulatory frameworks, a lack of skilled cybersecurity professionals, low digital literacy, and poor security infrastructure is identified and analyzed. This approach helps in understanding the root causes of cybersecurity in Africa.

The study also explores the dual role of AI and ML in the cybersecurity landscape. We review existing literature to understand how these technologies can both contribute to cyber risks—like automated attacks and advanced phishing techniques—and enhance cyber defense through threat detection, prediction, and incident response. Ethical considerations and the responsible use of AI in cybersecurity are also briefly discussed.

Finally the analysis find are used to create suggestion aimed at improving cybersecurity and privacy protection in Africa. These suggestions target strengthening of legal frameworks, improve digital infrastructure, enhancing education and training, raise public awareness, and encouraging regional and international corporations. This methodology offers a structured dependency foundation for understanding cybersecurity challenges and fostering secure digital growth in Africa. However , the study was certain limitations. The study depends on report cyber incidents, and underreporting may

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

skew the accuracy of the overall figures. Differences in national report standards and limited public disclosure of cyber breaches may also limit thorough comparative analysis.

IV. FINDINGS

This section presents the findings of the study based on secondary data collected from reports, research articles, and official sources related to cybersecurity and privacy challenges in Africa. The data covers cyber incidents, affected sectors, types of attacks, and regional distribution across North, East, West, and South Africa. Only factual information is reported here; no interpretation is included. Regional Distribution of Cyber IncidentsThe data shows a total of 1,250 reported cyber incidents across 11 African countries in 2024.

Table 1 summarizes the distribution by region:

Distribution of Cyber Incidents in Africa (2024)

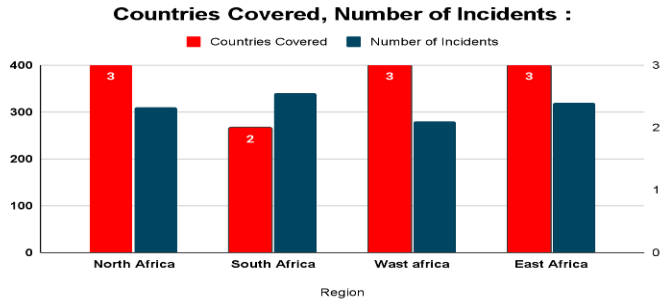
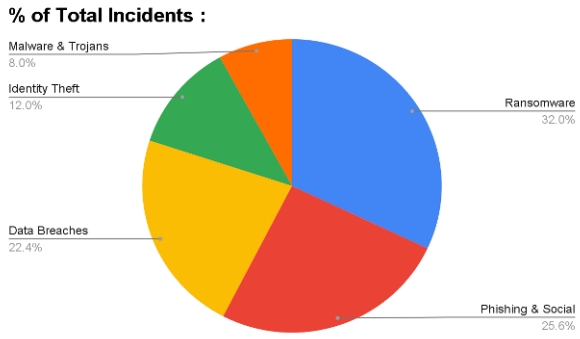


Figure 1: Regional

- **Cyber Attack Types**

The analysis identified the most common types of cyber attacks across Africa, as shown in Table 2:



- Figure 2: Percentage Distribution of Cyber Attack Types

1) 7.3 Sector-wise Cyber Incidents

Table 3 shows the distribution of cyber incidents across key sectors:

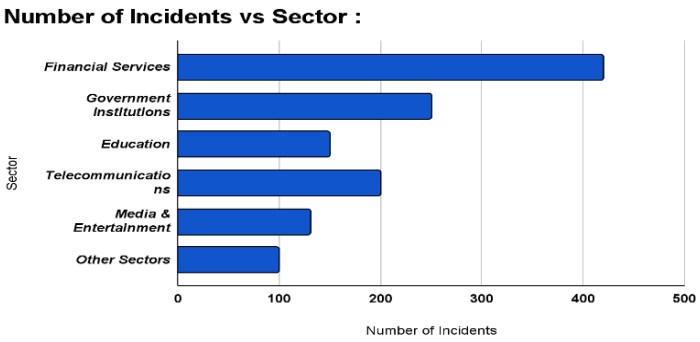


Figure 3: Sector-wise Distribution of Cyber Incidents

- **Cybersecurity Skill Shortage**

According to regional surveys, only **38% of African organizations** reported having adequately trained cybersecurity personnel, while **62% reported insufficient skills**. This is shown in **Figure 4**, a stacked column chart highlighting the skill gap across regions:

V. DISCUSSION

The study rescinded key points for cybersecurity in Africa for 2024. There were 1250 incidents reported in 11 countries. This reveals an increase in cyber threats, likely due to Africa's faster digitization. Areas with higher use of digital technology and mobile banking experienced more cyber incidents. As Africa continues to go digital, it is likely to face cyber issue. Addressing cybersecurity in Africa is essential. Cyber attacks come in different forms. The common type include phishing and social engineering attacks, followed by ransomware and financial fraud . Phishing attacks are widespread because many people lack knowledge about online safety. Such attacks typically occur through email, sms, and mobile applications. Many peoples number in africa use smart phones and mobile money platforms, which increases their vulnerability to phishing. Cyber attack, particularly phishing, pose a risk due to high phone usage.

The banking and financial services sector faces cyber incidents because it handles numerous transactions and sensitive data, and it is quickly expanding mobile money services. Government institutions are heavily affected. They often do not invest adequately in cybersecurity and lack

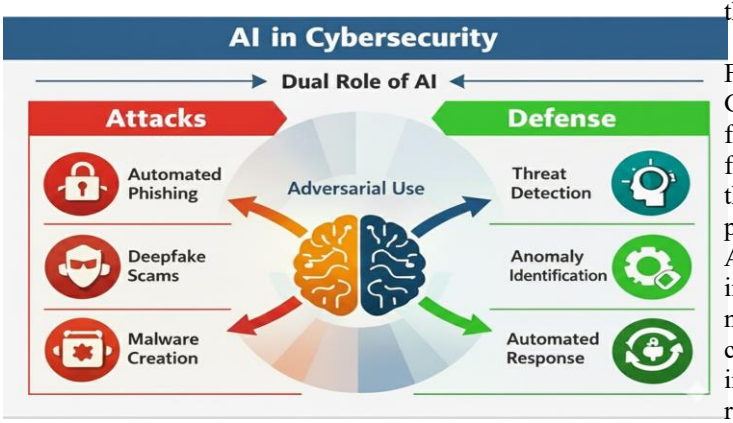
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

effective incident response systems. The telecommunications and digital service sectors are becoming more vulnerable as they increasingly rely on cloud services and deliver services online.

The study signified a significant problem: the lack of cybersecurity experts. The survey observed that only 38% of organizations have appropriately trained cybersecurity personnel, while 62% lack enough skilled workers. This situation hampers organizations' ability to monitor threats, respond quickly, and implement effective defenses. In regions with a deficit of cybersecurity skills, it takes longer to identify breaches and recover from incidents. This skills gap is a big challenge for cybersecurity.

Legal and regulatory challenges also exacerbate risks. Some African countries have established laws for cybersecurity and data protection, but these laws are irregularly implemented. The Malabo Convention has not been completely implemented, making regional cooperation difficult. Investigating cross-border cybercrimes is challenging due to Distinct national regulations and a lack of information sharing. While cybersecurity and data protection laws are crucial, these challenges complicate effective enforcement. The Malabo Convention is intended to enable cooperation, but inconsistent enforcement of its effectiveness in addressing cross-border cybercrime and cybersecurity risks.

Artificial intellegence and machine learning impact cybersecurity processes. They are misused to create fake emails and distribute them. They enable the production of realistic looking videos and images, complicating the work of security system. Conversely, these technologies can enhance cybersecurity, identifying potential security issue and allowing for the fastest response to unusual activities. In areas with limited resources, Artificials intelligence and machine learning can mitigate the scarcity of skilled personnel. Conversely, without proper regulation governing their use, these technologies also lead to additional problems. Determining the appropriate and ethical applications of AI and ML can be challenging.



Overall, the discussion highlights that Africa's cybersecurity issues are multifaceted, involving technological growth, regulatory gaps, a lack of skilled workers, and the emergence of AI-driven threats. Without coordinated policy enforcement, workforce training, and strategies for integrating AI, digital advancements may continue to exceed security preparedness.

VI. RECOMMENDATION

Based on our Insights, we have several suggestions to increase cybersecurity and privacy protection in Africa. These recommendations are for strengthening defenses in the region.

Governments need to assure that existing laws protecting individuals' information and data are strictly applied. While many more countries have established this laws, enforcement has been lacking. Governments should expedite the full implementation of the Malabo Convention to create a unified framework for cybersecurity and data protection across Africa. Second, investment in cybersecurity infrastructure is necessary. Systems that adopt Artificial Intelligence to monitor threats can significantly reduce response times and minimize financial losses, particularly in addressing prevalent issues like phishing, ransomware, and financial fraud. We need to tackle cybersecurity challenges alongside advancements in Artificial Intelligence.
Addressing the shortage of cybersecurity experts is essential. With a 62% skills gap, countries throughout the continent must collaborate to improve this situation. Governments and universities should develop educational programs emphasizing on cybersecurity and offer certifications to validate skills. Collaborating with companies to provide training can help fill this workforce gap.

Fourth, awareness of cybersecurity threats must be elevated. Given that phishing is a big risk, educating people about red flags such as suspicious links and promoting the use of multi-factor authentication and strong passwords can greatly reduce the potential of successful attacks. Raising awareness about phishing and its mechanics is vital for public protection.Fifth, Africa should establish regional platforms for sharing information about cyber threats. Since cyber threats cross national borders, countries can improve their defenses by collaborating and sharing threat information. A system for information exchange would significantly contribute to regional security.

VII. FUTURE SCOPE

Future research could offer further insights for this topic. By collecting data from businesses in various African nations and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

analyzing it, we can understand the connection between digital usage and cyber risk. Observing incidents over five to ten years will help predict future challenges**.** Research can also focus on developing cybersecurity models that use Artificial Intelligence to anticipate problems, specifically tailored for Africa's internet and computer systems. Given the limited resources and expertise in this field, models should reflect these realities.

Additionally, Evaluating Africa's progress with other Developing internet and computer system markets, such as certain countries in Asia or Latin America, could provide the lessons. This comparative analysis might offer new ideas for improving cybersecurity across Africa.

VIII. CONCLUSION

Africa is changing quickly in terms of digital technology. This shift as made a difference for people in Africa, allowing them to manage money better, communicate more easily, and join the economy. However, as Africa becomes reliant on digital tools, it faces the increased risks in africa. In 2024, there are 1,250 reported incidents across 11 African countries. The rise in cyber incidents is due to the rising dependency on digital answers.

The study reveals the phishing,ransomware, and finance related scams are the main issus. These threats primarily impact the banking and government sectors.a significant problem is the lack of skilled professional to handle cybersecurity. 62% of organizations report a shortage of qualified staff. In this issue it is compounded by inconsistent regulating and poorly enforced laws, these laws make it too challenging to defend against cyber threats. The gaps in cybersecurity workforce and regulatory practices are major concerns. The banking and government sectors remain the top targets for phishing, ransomware, and finance fraud. Artificial Intelligence and Machine Learning present these challenges and useful ways to protect ourselves. While AI can be used to carry out advanced cyber attacks, it can also assist in detecting threats and responding quickly. Therefore, we must implement AI responsibly when developing our cybersecurity methods. Considering AI and Machine Learning is vital as your address cybersecurity.

In this sustainable digital growth Africa needs a coordinational approach to include stronger and legal enforcement, AI based defense systems and public awareness program. Without this all measures digital growth may continue to outstrip our cybersecurity readiness.

IX. REFERENCES

[1] International Telecommunication Union Global Cybersecurity Index 2023,Geneva,2023.
[2] African Union, African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), Addis Ababa,2014.
[3] Interpol, African Cyberthreat Assessment Report 2023,Lyon,2023.
[4] World Bank, Digital Economy for Africa Initiative (DE4A),Washington, DC,2023
[5] United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide,2023.
[6] S. M. Furnell and M. Karweni, Security implications of electronic commerce: a survey of consumers and businesses, vol. 9, no. 5, pp. 372, 382, 1999.
[7] [7] M. Mutungi and J. P. Mtsweni, Cybersecurity challenges in Africa: An analysis of the current threat landscape, African Journal of Information Systems, vol.12, no. 4, pp. 45, 60, 2020.
[8] [8] A. Aborode et al., “Cybersecurity threats in Africa: Trends and mitigation strategies,” Journal of Cyber Security Technology, vol. 6, no. 2, pp. 85, 102, 2022.
[9] [9] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” Computers & Security, vol. 38, pp. 97, 102, 2013.
[10] [10] B. M. Dzomira, “Digital financial services and cybersecurity risks in developing economies,” International Journal of Economics and Finance Studies, vol. 13, no. 1, pp. 112, 130, 2021.
[11] [11] A. Taddeo and L. Floridi, “The ethics of artificial intelligence in cybersecurity,” Philosophy & Technology, vol. 31, no. 3, pp. 1, 15, 2018.
[12] [12] S. Makinde and T. Shorunke, “Artificial intelligence in cybersecurity defense systems,” International Journal of Computer Applications, vol. 183, no. 21, pp. 15, 22, 2021.