THE USE OF ARTIFICIAL INTELLIGENCE (AI) TO MANAGE CYBER FRAUD INCIDENTS IN THE NIGERIAN FINANCIAL SECTOR

HARRISON OZAH

MYKOLAS ROMERIO UNIVERSITY

ABSTRACT

The increasing number of cyber incidents has highlighted the urgent need for innovative solutions to enhance cybersecurity within Nigeria's critical infrastructure and financial sector. Artificial intelligence (AI) models have emerged as essential tools in combating cybercrime, particularly as human error continues to expose vulnerabilities and lead to significant losses in these sectors. However, the question remains: can AI models effectively mitigate these risks? This study examines the use of AI models to manage cyber incidents within Nigeria's critical infrastructure and financial sectors.

A quantitative research design was adopted, employing a survey method to collect primary data from a sample of 218 IT specialists working in both the private and public sectors, specifically within Nigeria's critical infrastructure and financial industries. The survey yielded a 71.7% response rate, with 18.3% of questionnaires left incomplete. Data analysis was conducted using SPSS software, with inferential statistics, including Chi-square tests and standard deviation, to assess the variance and test the hypothesis regarding the effectiveness of AI models in managing cybercrime incidents.

The findings suggest that organizations within Nigeria's critical assets and the financial sector are increasingly adopting AI solutions, such as predictive analytics and behavioural analysis tools and others, to effectively address cybercrime incidents. Respondents expressed positive sentiments, indicating general agreement about the successful implementation and effectiveness of AI technologies within their organizations in quick responding resolutions and protecting of critical assets and the financial sector in cyber incidents. However, this indicates, the need in some areas of AI model limitation that requires human decision due to increase number of false positive flagging.

INTRODUCTION

The relevance of the study: The rapid and widespread use of cyberspace has had a profound impact on modern life, affecting our fundamental rights, social interactions, and economic activities, all of which rely on seamless digital communication technologies. This digital transformation has eliminated barriers between countries, institutions, and individuals, enabling global interactions and the exchange of information.

While the benefits of digital spaces are undeniable, they come with inherent risks. Design flaws and the criminal tendencies of cyber attackers exploit vulnerabilities in critical assets (Humayun et al., 2020). Daniel et al. (2017) defines cybersecurity as a comprehensive collection of tools, techniques, policies, measures, and strategies, including the use of the latest technologies, to safeguard cyberspace and its users' assets. Other

definitions emphasize protecting both the physical and non-physical components of organizations from unauthorized access.

The growing number of cybercrime incidents worldwide has underscored the urgent need for defensive tools that target vulnerabilities and risks that could undermine the effectiveness of cyberspace. For example, the 2021 Africa Cyberthreat Assessment Report estimated that cyber fraud in the region had a financial impact exceeding $4 billion, representing about 10% of Africa's total GDP (African Intelligence, 2024). This problem has only worsened since then, with increasingly complex cyberattacks targeting government infrastructures, hospitals, financial institutions, and internet service providers.

In Nigeria, and globally, cybercriminals primarily exploit human error through sophisticated social engineering techniques. Attacks like phishing, ransomware, and scams target social media, instant messaging platforms, and other communication channels. Despite proactive government efforts to secure cyberspace, traditional methods have proven inadequate. Therefore, exploring advanced approaches, such as artificial intelligence (AI), is essential for managing and preventing cybercrime. This study aims to investigate the use of AI to combat cyber fraud in Nigeria's financial sector and other critical assets.

Novelty of the study: Today our society is highly dependent on internet and other advanced information technology tools for performing various business activities and benefits. While these venture is seen a good development for productivity, efficiency and communication, They also aline with pains to governments, institutions, businesses, individuals, banks and other services. According to the U.S. Federal Bureau of Investigation, reported cases of cyber fraud in the first quarter of 2024 surged significantly. In 2021 alone, cyber fraud complaints reached a record 880,418 from the American public, with potential losses exceeding $12.5 billion. This represents a nearly 22% increase in both complaints and losses compared to 2022. While many countries, institutions, and regions are proposing policies to curb the rise of cyber fraud in critical sectors like healthcare, finance, and the national economy, efforts continue to fall short. For example, on April 23, 2023, the European Union proposed the EU Cyber Solidarity Act, aimed at improving response mechanisms to cyber fraud across Europe and its member states. This proposal includes a European security shield and the establishment of cyber emergency units to strengthen defenses against cyber fraud attacks.

Despite the various programs being implemented by national governments to safeguard cyberspace, cyber fraud continues to be a persistent global threat. There is a growing need for more proactive measures and advanced technological tools, as reliance on traditional and conventional models has failed to address the existing gaps. While numerous studies on cybersecurity have been conducted globally, limited research has focused on the application of artificial intelligence (AI) to combat cybercrime within the specific context of Nigerian society and its financial sector, leaving this area largely underexplored.

While several studies in Nigeria have examined cybersecurity management, technological advancements have shown that AI and machine learning are gaining wider acceptance than human intervention in preventing cyber fraud in Nigeria’s economy and financial sector. However, most studies have focused on the benefits and challenges of AI in preventing cyber fraud, without considering other critical sectors, particularly the financial sector, which remains significantly impacted by cyber fraud incidents. Meraj. Et.al (2022) on impact and limitations, Des and Sandhane (2021) on the management of cybersecurity. Montasari and Hill (2019) on the

challenges and Becue (2021) on opportunities and challenges. This study intend to explore the gap created in this field while using artificial intelligence to prevent and manage cyber fraud attack in the Nigerian financial sector.

Statement of the problem: The escalating rate of criminal activities in cyberspace has become alarming, with cyber fraud encompassing a wide range of illicit activities and posing a pervasive global threat. The growing reliance on internet services for business operations, banking, healthcare, e-commerce, and communication has provided cybercriminals with new opportunities to expand their reach, and Nigeria is no exception. Despite these challenges, implementing defensive measures such as residential proxies, strong password protocols, and vulnerability assessments remains essential. The complex nature of cyber fraud demands a comprehensive and proactive approach to cybersecurity. Advanced, forward-thinking strategies are crucial in an era where the digital world is as critical as the physical one, highlighting the need to stay ahead in an ever-evolving cyber landscape.

According to a United Nations report, cyber fraud incidents have cost the global economy an estimated $1.5 trillion. This figure is based on historical cybercrime data, recent year-over-year growth, and the dramatic increase in hacking activities by hostile nation-state actors and organized crime groups. The Budapest Cybercrime Convention (2001) adopted a broad framework for gathering evidence in cybersecurity, setting a precedent for international cooperation. However, stakeholders in the financial sector view cyber fraud incidents as a significant challenge to growth and profitability (Vieira and Seghal, 2018). Balaji (2021) emphasizes that cybersecurity is critical for the financial sector, as it is frequently targeted by cybercriminals seeking to access victims' accounts, steal depositors' funds, and commit other financial crimes. The increasing use of sophisticated hacking techniques and successive breaches of the national economy and financial sectors have sparked debates on information security and privacy protection. As physical infrastructure and other assets in the financial sector become more vulnerable to cyber fraud and other threats, there is a pressing need for a more reliable cybersecurity model that can detect unusual behaviour and mitigate risks effectively.

Artificial intelligence (AI) is seen as a new model for dectection and prevention of series of cyber fraud incidents using real-time algorithm decision. Human intelligence to prevent cyber fraud attack is becoming inefficient and effective (Kose, 2019). Most cyber fraud incidents are performed by intelligent agent's computer viruses, ransomware, and worms , to combat these challenges an intelligent automated agent needs to be produced, to detect, evaluate, and respond to cyber fraud incidents in the financial sector to avoid bridges in compliance with regulatory agencies in real-time. Thereby emphasizing the need and significance of the subject, a research problem is identified to conceptualise the use of artificial intelligence (AI) to manage cyber fraud attack and fill in the gap created in empirical work on the use of artificial intelligence (AI) in the fight against cyber fraud attack in the Nigerian financial sector where human expertise and conventional model has failed.

The main research question: In today's world, digitalization has become inevitable and is now a key driver of information sharing. Health services, financial institutions, government agencies, and individuals all rely on the benefits, as well as face the challenges, of the digital space. Cyber fraud incidents have risen

exponentially alongside the rapid growth of cyberspace. The widespread use of internet applications in almost every aspect of daily life is a major contributor to this increase.

Governments, individuals, and businesses are now expected to develop models that prevent cyber fraud incidents, protecting both physical and non-physical assets. In this context, embracing artificial intelligence (AI) models over traditional manual approaches is becoming essential in combating cyber fraud in Nigeria's financial sector.

The central research question is: Can AI models effectively prevent cyber fraud incidents in Nigeria's financial sector and society, despite the continued rise in cybercrime?

The Object of research: The use of artificial intelligence (AI) to manage cybercrime incidents

The Aims of the study: To examine the use of artificial intelligence in. the prevention of cybercrime in Nigeria critical assets and the financial sector.

The Objectives of the study: The research shall pursue the following objectives, examine the theoretical aspect and empirical testing of using artificial intelligence (AI) in the fight against cyber fraud incidents in Nigerian society and the financial sector:

1. To examine the theoretical aspect of using artificial intelligence model in the prevention of cyber fraud incidents.
2. To identify major cybercrime incidents in the Nigeria critical asset and the financial sector.
3. To evaluate AI model in the fight of cybercrime incidents in Nigeria critical assets and the financial sector.
4. To explore the type of AI model currently being utilized to mitigate risk in cybercrime incidents in Nigeria critical assets and the financial sector.

The research method: A quantitative research strategy will be adopted in this resaerch study, and a statistical secondary data used in our study analysis. The quantitative research strategy is used to determine the effect of artificial intelligence models (AI) in the prevention of cyber fraud incidents in the Nigeria society and the financial sector. A case study design is chosen in this study because it gives the researcher in-de[th knowledge and information about the participants in the study. It is unbiased, efficacy, reliable and valid in the outcome. Other studies such as Montasari and Hill (2019), Des and Sanhane (2021) and Meraj et.al (2022) justisfy the use of the quantitative research strategy using descrptive statistics in their study analysis outcome.

A survey method shall be used in the study where questionnaires shall be designed and distributed to the participants online to inputs their opinion on the use of artificial intelligence in the fight against cyber fraud incidents in the Nigeria and the financial sector.

The Scope of the Study: This study explores the application of artificial intelligence (AI) in managing cyber fraud incidents and crime within the Nigerian financial sector and other critical infrastructure. The study focuses on identifying how AI technologies, such as machine learning algorithms, predictive analytics, and automated response systems, can be employed to enhance the detection, prevention, and response to cyber threats. The research will examine existing AI frameworks and models used in the financial sector, evaluate their effectiveness in mitigating cyber fraud, and assess their applicability in the Nigerian context.

Additionally, the study will analyze the challenges associated with integrating artificial intelligence into cybersecurity management in Nigeria.

Limitation of the Study

1. The study may be limited by the availability of relevant and comprehensive data on cyber fraud incidents within the Nigerian financial sector. Access to proprietary data from financial institutions may be restricted due to confidentiality concerns.
2. Nigeria's technological infrastructure may pose limitations in the adoption and implementation of advanced arificial intelligence systems. The study may not fully account for the disparity in technological capabilities between urban and rural areas.
3. The rapidly evolving regulatory landscape in Nigeria concerning AI and cybersecurity might limit the scope of the study. The application of artificial intelligence applications is new.
4. While the study focuses on the Nigerian financial sector, the findings may not be entirely generalizable to other sectors or countries with different regulatory, technological, and economic contexts.

Theoretical implications of the study: shows the following could be achieved in the study

1. This study contributes to the theoretical understanding of how artificial intelligence can be integrated into cybersecurity frameworks, particularly in the context of developing countries like Nigeria. It provides insights into the capabilities and limitations of artifical intelligence application in detecting and preventing cyber fraud incidents.
2. The study will contribute to the development and refinement of artificial intelligence-based cybersecurity models that can be adapted to the unique challenges of the Nigerian financial sector.
3. The study will theoretically give details how artificial intelligence-driven behavioral analysis and predictive analytics can anticipate cyber threats, contributing to the broader field of cybersecurity risk management.

Practical implication of the study: indicate the following could be achieved from the research findings

1. The findings of this study could help financial institutions in Nigeria to enhance their cybersecurity strategies by adopting Artificial intelligence advancement, leading to more effective management of cyber fraud incidents.
2. Insights from the study can inform policymakers and regulators in Nigeria about the benefits and challenges of integrating artificial intelligence model into the financial sector’s cybersecurity framework. This could lead to the development of more robust regulations and standards for AI use in cybersecurity.
3. The study will enable Financial institutions to optimize the resources from the findings to guide against more complex threats.

By addressing these areas, the study aims to provide empricial findings on the use of Artificial intelligence in managing cyber fraud incidents in Nigeria, offering both theoretical insights and practical recommendations for stakeholders in the financial sector and Nigeria national cybersecurity

1.0 THEORETICAL ASPECT OF ARTIFICIAL INTELLIGENCE IN THE PREVENTION OF CYBER FRAUD INCIDENTS

This chapter examines the use of artificial intelligence (AI) model in managing of cyber fraud incidents in Nigeria critical asset and the financial sector. Its analysis the impact of artificial intelligence and contributions of other scholars as it relates to the theoretical aspect and empirical works from past to present in the use of artificial intelligences in the management of cyber fraud incidents. Also, it defines the concept of cyber fraud incidents and artificial intelligence, the impact on Nigerian critical assets and the financial sector. The model design in the management of cyber fraud incident and legal framework of Nigeria, as it relates to other counterparts. This chapter evaluate the theoretical and empirical findings of various scholars on the effect of artificial intelligence application in cybercrime prevention incidents.

1.1 INTRODUCTION

The growing reliance of national economies, businesses, and individuals on digital advancements and infrastructure for business and financial transactions has heightened the risks associated with cybercrime. Cyber fraud incidents are becoming more frequent, widespread, and damaging to the development of the digital economy. This underscores the need for AI-driven cybersecurity measures and the likely impact in managing the Nigerian critical assets and the financial sector. Various research has linked these cyber threats to nation-state actors and criminal organizations, targeting infrastructure vulnerabilities (Herley, 2010). To protect critical assets in cyberspace, there is a pressing need for a combination of devices, protocols, and practices that prevent fraud, unauthorized access, and damage to networks, systems, software, and data, which has led to the call for the use of artificial intelligence applications in managing cybercrime incidents.

Cybercrime incidents have been a big challenge globally as perpetrators often target internet platforms for unlawful gains and access to individual sensitive personal and financial information of the victims, institutions and governments (Afolayan, et.al 2015). Advisory bodies like National institute of Standard and Technologies (NIST) have been pushing for the implementation of a more proactive and flexible strategies that focus on data-driven analysis, that will detect, identify, and avert event of future cyber fraud incidents in national economies of countries.

Cyber fraud incidents have been malicious to the global business and Nigeria is not exempted. The impact is enormous on critical infrastructures and the financial sector. The actors use technological advancement devices to penetrate these actions for personal economic benefits (Owolabi, 2010). The implementation of artificial intelligence tools in the Nigeria critical infrastructures and financial sector is a need. Empirical studies have not truly shown the likely impact of artificial intelligence application in managing cybercrime. Some studies such as Gautam (2023) describe the application as multifaceted. The advanced algorithms enable more sophisticated credit risk assessment models by identifying subtle patterns in large data sets, often

unnoticed by humans. Artificial intelligence plays a sequential role in automating compliance with regulatory norms, thereby reducing human error and ensuring swift adaptation to regulatory changes.

Maitanmi (2013) defined cyber fraud incidents as a type of crime performed by fraudsters using a computer device and the internet as a connection to reach out to their financial objectives.

Solomon et.al (2022) further described it as using computer or mobile devices as a tool, and internet to achieve illegal objectives such as fraud, phishing, identity theft, attacks and digital signature forgery.

However, the definition proposed by most scholars are similar in terms, but authors like (Payne 2020) definition affirm to the use of computer, mobile and internet devices as a component of digital advancement in the penetration and unlawful access of the victim personal information but further explained that the success is due to human error and vulnerability. The definition as shown the need of artificial intelligence (AI) as a tool in the management of cyber fraud incidents.

1.2 THE CONCEPT OF ARTIFICAL INTELLIGENCE

In today's businesses, artificial intelligence has been incorporated into the cybersecurity systems of most business in a range of functions to support human security. The capabilities of the artificial intelligence are expanding at a never-before-geometric progression. These technologies have a range of useful applications such as behavioral analysis and machine translations. However, artificial intelligence is a fascinating technology that can easily analyze millions of events, track different ranges of cyber activities, analyze information to protect against constantly evolving cyber fraud incidents in our national economies, businesses and individual critical asset. Artificial intelligence date back to the 1950s with several progression to make it relevance in our today digital advancement through research studies.

Alan Turing (1950) was the first to discuss computing machinery and intelligence in his book in which he presented the methodology for evaluating machine intelligence., Which was the light for the early stages of artificial intelligence.

John McCarthy (1956) The father of the artificial intelligence who made the word "artificial intelligence" went further to explain it is the combination of science and engineering to make intelligence device for human welfare. He went more to say artificial intelligence is an intellect, that is much sharper than the best of human brain in the real-world including computer science and linguistic logic. It is an improved model of machine learning which can do muscle work and demonstrate in intellectual manner to solve difficult problems. It starts with basic and most vital aspects of our life like philosophy, computer science, mathematics, linguistics, neuron science and sociology.

Keplan et.al (2019) broaden the term artificial intelligence that the system can rightly interpret external data, learn from the data and use those learning to achieve certain aim and duties through a flexible adaptation system. They are also of the view that it can be divided into three stages, analytics, human inspired and humanized. The human inspired. Artificial intelligence has the consistency of cognitive and emotional intelligence by understanding human emotions and the use of these credentials in its decision making. At the

humanized level, artificial intelligence exhibits feature of all type of competence both cognitive, emotional and social intelligence and can be self-aware in interaction.

The US Department of treasury (2024) further gave a better understanding of the concept "Artificial intelligence" They defined it as a machine-based system that can make decision, suggestions and forecast that affect real- virtual environments given a set of human and defined objectives. Artificial intelligence system sense both real and virtual surrounding using machine and human based inputs. They automatically analyze and abstract these perceptions into models and use the inference to create information and actions.

Though the definitions illustrate that Artificial intelligence applications in cybercrime prevention has its practical impact. Artificial intelligence system analyses vast amounts of financial data, identify fraudulent patterns and detect anomalies in real-time, enabling early intervention and mitigating financial and reputational damage. AI-driven applications prevent unnecessary access, with the use of machine learning and natural language processing to monitor and analyze financial activities and communications, by staying ahead of evolving cyber threats and enhancing the security of the critical assets and the financial sector. (Urbas, 2019)

1.3 TYPES OF CYBERCRIME INCIDENTS IN NIGERIA CRITICAL ASSET AND THE FINANCIAL SECTOR

Cyberspace usage has grown exponentially over the past two decades, expanding from 500 million users to approximately 5.44 billion users worldwide in 2024 (Forbes Home, 2024). As globalization continues, the growth of digital spaces has now outpaced regulatory tools, leading to the emergence of new criminal groups and challenges in policing cyber fraud incidents globally. Cyber fraud manifests in many forms, yet there is no standardized way of conceptualizing it, and the lack of a clear definition complicates efforts in prevention and remediation (Mabunda, 2017). Cyber incidents is more complex to define than traditional crimes due to its methods and reliance on computers, the internet, and other advanced tools. The crime may occur on a computer device or even in an offline location (Mabunda, 2017). Another definition suggests that cyber fraud refers to the use of computer components to initiate criminal activity (Payne, 2020).

More broadly, cyber fraud can be understood as any act of deceit using internet and computer technologies to defraud the public of personal assets, data, money, security, and services (Urbas, 2019). These incidents compromise the confidentiality, integrity, and availability of computer data and systems, contravening the Budapest Convention on Cybercrime (2001).

Cyber fraud attacks are often large-scale and targeted at critical assets, as seen in notable cases such as the 2007 cyber-attacks on Estonia and the 2014 attacks in Ukraine (Schjolberg, 2008). The advent of artificial intelligence (AI) has transformed the landscape of protecting both public and private critical infrastructure against cyber threats. The use of machine learning to predict and prevent denial-of-service attacks on critical assets has been impactful (Hernandez-Castro et al., 2014). AI applications have also enhanced transparency and security in social and financial activities, including in recent elections such as the 2014 Ukrainian and the 2023 Nigerian presidential elections, helping to prevent cyber interference (Nwankwo et.al, 2023).

However, malicious actors have also adopted AI to exploit vulnerabilities in both digital and physical assets, causing significant damage to systems. Studies, such as those by Christian et al. (2023) and Qiang and Yiqian (2010), highlight the potential for AI misuse in targeting critical assets, particularly in the financial sector, despite substantial investments in AI for infrastructure protection (Gumbi, 2018). Modern AI-driven identity crimes like deepfake technology are increasingly used in cyber fraud, enabling attacks on individuals and organizations through hacking, ransomware, advance fee scams (like the "Nigerian scam"), fake websites, and payment fraud.

One notable case highlighted by the United States Attorney's Office involved a civil forfeiture action to reclaim $5.3 million tied to a business email compromise scheme that defrauded a Massachusetts workers' union. Cyber actors used AI-generated emails in a spoofing attack that tricked the union into transferring $6.4 million to fraudulent accounts routed through foreign banks and cryptocurrency exchanges. This incident exemplifies the potential for AI-enabled social engineering attacks on critical infrastructure.

This study will evaluate the most current and pervasive types of cybercrime incidents, particularly in Nigeria's critical assets and financial sectors, to explore the role of AI in managing and preventing cyber fraud.

1.3.1 MALWARE INCIDENT

Various studies have demonstrated that malicious software is one of the most significant cyber threats, designed to damage, disrupt, and gain unauthorized access to computer systems. As the complexity of malware incidents increases, the application of artificial intelligence (AI) has become crucial for detecting malware-related cyber-attacks. According to Saxe and Berlin (2015), their study illustrates how deep learning can be applied to malware detection by converting binary program features into a format suitable for neural network analysis. The authors note that deep learning models, when trained on large datasets of malware samples, can detect and classify malware more accurately than traditional methods.

Additionally, Canali et al. (2014) demonstrates the effectiveness of AI in analysing network traffic and identifying malware based on unusual behaviour patterns, rather than relying solely on traditional signature-based methods. By focusing on network anomalies, their results indicate a proactive approach to threat detection. However, other studies highlight the challenges and limitations of using machine learning and AI in detecting malware attacks, such as those by Papadopoulos et al. (2021) and Souri and Hosseini (2018). These researchers advocate for the integration of AI with human expertise to address these issues and call for more adaptive models to enhance detection resilience.

1.3.2 PHISHING SCAM INCIDENT

The rise of phishing scams poses significant challenges to individuals and organizations alike. However, the integration of artificial intelligence into phishing detection and management offers promising solutions. Phishing attacks involve fraudulent emails and messages that mimic legitimate sources to tricking users into clicking on malicious links and attachments. According to Jain et al. (2019), these attacks use social engineering tactics to manipulate victims, often leveraging fear, curiosity, and urgency to prompt immediate action. Several studies have shown the impact of artificial intelligence tools to analyse reported phishing sites

and enhance detection algorithms. According to Mavridis et.al (2023) the use of machine learning capabilities mitigates phishing threats through natural language processing and anomaly detection technique. By establishing baseline patterns for normal activity, AI systems could flag any deviations that may indicate phishing attempts. As noted by Hu et al. (2022), this proactive approach allows organizations to detect phishing scams before they result in significant damage. Additionally, Google enhances user security by providing real-time alerts and blocking malicious content (Google, 2021)

1.3.3 ONLINE AUCTION FRAUD

The proliferation of online marketplaces has led to a rise in cyber fraud, particularly in auction environments. Common forms of cyber auction fraud include misrepresentation of items, illegitimate bidding practices intended to manipulate prices, and hidden charges, such as inflated shipping and handling fees (Gururaj et al., 2024). Additionally, incidents involving non-delivery of items, the sale of black-market goods, and fraudulent online payment transactions contribute to the complexities faced by consumers. A frequent complaint from buyers includes false payments, often facilitated with stolen or forged checks, as well as accounts with insufficient funds to cover transactions (Gururaj et al., 2024). According to Mosli et.al (2017) AI technologies have emerged as essential tools for detecting and managing online fraud in auction settings. By leveraging machine learning algorithms and data analysis techniques, AI can identify suspicious patterns indicative of fraudulent activities. Evaluating the financial health of the accounts involved, AI systems can also flag transactions that present red flags, such as insufficient funds, thus preventing fraudulent payments from being processed which makes it significant in detecting online market transaction.

1.3.4 PHONY WEBSITE FRAUD

The process of buying goods and services directly online without a bid. Recently individuals have become increasingly sophisticated at replicating websites and consumer products. They collect confidential information, extract economic resources from consumers and offering services and goods without being of promised quality. The increased use of lucrative software products has made individuals and businesses to be easily tricked to this unsecured website to steal card data and other personal data.

1.3.5 NIGERIA SCAM KNOWN AS 419 ADVANCE FEE FRAUD INCIDENTS

The term “419” of the Nigerian cybercrime attack criminal code (Nabiebu et.al 2024). The scam which is called “advance fee fraud” began with offenders frequently working from Nigeria and targeting victims across the globe usually with letters sent through the postal service mail. The cyber fraudster liaises with other partners within other jurisdiction such as African, US, Canada and Britain to perfect the cybercrime incidents against the victim. It requires the victims to pay the scammer in advance with the promise of obtaining a highly lucrative reward in form of a cheque benefit and heritance gift (Brody et.al 2022). The cyber incident comes with a spam message from a foreigner who needs help moving millions of dollars out of his homeland and offer the victim a certain percentage of the fund when assisted in the transfer. The fraudster asks the victim for a pay request to secure the offer benefit. The scam is actualized a long process of interaction and trust with the victim in which the target becomes engrossed to the plot and conned by the scammer’s ability to establish sympathy, rapport and trust without ever meeting in physical contact (Brody et.al 2022).

1.3.6 DEEPFAKE

According to Xuan et al. (2019), deepfakes represent one of the biggest recent challenges in managing cybercrime with artificial intelligence. Deepfakes are commonly used in cyber fraud incidents by employing falsified identification documents and using AI tools to misrepresent identity, voice, and other personal information. This technology leverages digital manipulation of audio, video, or images through generative adversarial networks (GANs), enabling the alteration of visual and audio content to create highly realistic, deceptive media. Research shows that deep learning techniques make it possible to generate content that appears authentic, which poses significant risks for AI applications in combating cybercrime (Laas, 2023). However, some studies, including Li and Lyu (2019), Afchar et al. (2018), and Verdoliva (2020), also highlight the positive role of AI tools in detecting deepfakes within sectors like finance, using advanced audio-based GANs, voice synthesis technologies, and trained detection algorithms

1.3.7 DARKNET MARKET

The darknet is a segment of the deep web that remains hidden and is inaccessible through standard web browsers. According to Andrei et al. (2024), it is used for both legal and illegal purposes, reflecting its dual nature enabled by its anonymity. Access requires specific software, configurations, and authorization. For instance, Tor anonymizes users by routing internet traffic through a global network of relays to obscure users' locations and activities from surveillance and traffic analysis. Similarly, I2P establishes layers of anonymity by directing traffic through a volunteer-operated network. The term "onion routing" refers to multiple layers of encryption, which reveal only the next step in the transmission process, ensuring that no single point knows both the source and destination of the data. Artificial intelligence (AI) has emerged as a crucial technology in combating cyber fraud in darknet markets. Research indicates that AI applications are essential in managing darknet-related incidents, though challenges persist. The constant evolution of the darknet, encrypted communication, and sophisticated obfuscation techniques make it challenging for AI to manage incidents fully. Noriega et al. (2020) argue that human expertise is critical alongside AI tools to interpret complex datasets and develop adaptable AI models for the continually evolving cybercrime landscape.

1.3.8 DENIAL OF SERVICE INCIDENT

A Denial-of-Service (DoS) attack is designed to disrupt the functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate requests, rendering it inaccessible to legitimate users. A Distributed Denial-of-Service (DDoS) attack intensifies this disruption by using multiple compromised systems to launch the attack simultaneously. Several studies highlight the impactful role of AI in managing DoS/DDoS incidents, from machine learning-based anomaly detection to real-time adaptive defenses. Such as, Reddy and Iyer (2023) discuss the potential of reinforcement learning to develop adaptive defenses against DoS/DDoS attacks, particularly in cloud environments. These AI-driven defenses can dynamically adjust to evolving attack patterns, providing a more flexible response than traditional fixed-rule approaches. Additionally, Gupta et al. (2020) analyses the challenges of AI in DDoS detection, such as adversarial attacks, data imbalance, and the need for continuous model updates. Their study emphasizes the importance of hybrid models and the integration of human expertise to enhance resilience against sophisticated attack methods.

Artificial intelligence driven cybersecurity model has come to offers a promising solution for prevention of cyber fraud incidents through improved detection, driving operational efficiency and combating artificial intelligence-based incidents (Sasmal, 2021). These models have shown impact in threat management by analyzing large datasets for patterns and anomalies thereby identifying fraudulent activities that might be missed by the traditional model. Several studies have shown AI defenses against cybercrime incidents such as DDoS, darknet market, deepfake and other. (Reddy and Iyer 2023), has made significant impact in using reinforcement learning in detecting unusual behavior and patterns. According to Noriega et al. (2020) argue that human expertise is critical alongside AI tools to interpret complex datasets and develop adaptable AI models for the continually evolving digital landscape. Noriega et al. (2020) argue that human expertise is critical alongside AI tools to interpret complex datasets and develop adaptable AI models for the continually evolving digital landscape. According to Noriega et.al (2020) that human expertise is critical alongside AI applications to interpret complex datasets for adaptability to the continued evolving cybercrime landscape. However, some studies have shown that AI application can be used against AI making the model a big challenge in managing cybercrime incidents such as Gupta et.al (2020), using adversarial attack and data imbalance give AI application a negative picture in protecting against cybercrime incidents.

A lot of studies of has shown variant significant impact of AI applications in managing cybercrime incidents in terms of critical assets of individuals and the financial sector such as Afchar et.al (2018), Li and Lyu (2019) and Verdoliva (2020) have all attributed the positive aspect of artificial intelligence model in their studies in the fight against cybercrime using advanced machine learning in predicting, identification, verification of clients, and analysing various advance threats in cybercrime. They also advocate for the use of AI applications combine with human expertise to examine large set of complex data for the changing landscape of cyber threat incidents across. Although AI-driven cybersecurity models, including real-time anomaly detection and behavioural analysis, are essential in combating these threats, but they must continuously evolve to remain effective. Countries like Nigeria need to invest in these advanced artificial intelligence-based security systems to manage the growing cyber risks

1.4 MODEL TECHNIQUE OF ARTIFICIAL INTELLIGENCE IN CYBERCRIME MANAGEMENT

The emergence of a novel technology of artificial intelligence has made it possible for cyber attackers to refine their techniques. Cyber threat has become more varied ranging from social engineering schemes to ransomware attacks. The introduction of artificial intelligence tools in managing cybercrime is a necessity in our public and private critical infrastructure.

The Budapest convention (2001) define cybersecurity as a safeguard and action that are put in place to protect the cyber domain from threats both in individuals, organizations and national economies that are associated with harm to the independent networks and information infrastructure, to give availability, integrity of the network and infrastructural confidentiality. According to Canali et.al (2014) Artificial intelligence application is revolutionizing the way to detect and prevent malware incidents. Various studies such as Wang et.al (2024) Singh et.al (2017) and Odumesi (2014) have demonstrated the significance of artificial intelligence tools to enhance cybersecurity efforts through automation, pattern recognition, and predictive analysis to protect and

prevent vulnerabilities of AI adversarial incidents. However, studies have discussed the limitations to AI in managing cybercrime incidents because of the over reliance of algorithms of datasets to learn and identify patterns that indicate malicious behavior and variant of new dataset of malware attack. It challenging and evident from past and recent research findings that AI model have been effective significantly in wading and protecting cybercrime incidents irrespective of the type of variant that occur.

Though developing an Artificial intelligence tool is a necessity in the evolving cybercrime on critical asset and the financial sector. Studies have shown the evolving trend of cybercrime in the Nigeria financial sector and the need to create a protective artificial intelligence tool to enhance cybersecurity and protect critical assets.

The components of the artificial intelligence model design for cybercrime protection:

1. **Data collection and integration**

The integration of machine learning tools in malware incidents, the algorithms will comprehensively collect the dataset, analyze, and integrate the system with other sources like network traffic, users' activity log and system events. While integrating the diverse data, it will perform a holistic view of the network environment. According to Marques et.al data collection integration should be centralized for the mobile intelligent multi agent system to function effectively in identifying and mitigating against cyber threat such as DDoS attacks by correlating data across different vectors.

1. **Anomaly detection**

The anomaly detection involves identifying deviation from the normal pattern of behavior within the network. The artificial intelligence and machine learning algorithm excel to detect these anomalies by analyzing large amount of data and recognizing the pattern that might elude the traditional model. Qiang and Yiqian 2010) demonstrated that the effectiveness of an artificial intelligence system base model is a real time anomaly detection by providing a timely alert for potential security breaches.

2. **Behavioral analysis**

The algorithm makes behavioral analysis by understanding the normal behaviors of the users and the systems to detect deviations indicative of malicious functions. The approach is critical in the performance of artificial intelligence security agent in identifying insider's threats and sophisticated external attack. Collins et.al (2021) studies provided evidence on the use of intelligent security agent in power grid protection which monitor and analyzes behavior patterns to detect intrusive acts.

3. **Predictive analytics**

The algorithm uses predictive analytics to make historical data. Machine learning forecast potential cyber threat before they occur. The model identifies trends and potential vulnerabilities, The predictive model enables proactive approach to decision making. Mohammed et.al (2024) and Solomon et.al (2022) showcase the significant impact of predictive analytics in enhancing cybersecurity by anticipating and mitigating risk.

The model is a forward-looking approach for preventing cybercrime incidents and minimizing the impact of attack. It claims efficiency, scalability and ease of diffusion but has it own shortfall due adversarial vulnerabilities.

4. Response automation

The model adopts response automation behavior using artificial intelligence model to automatically respond to detect threats without human intervention but needs human decision-making support for analysis. This requires isolating compromised systems, blocking malicious traffic and initiating incidents response protocols. Marques et.al (2024) studies demonstrated the significance of automation while adopting multi-agent system for combating DoS attack showcasing the potential of artificial intelligence model to manage cyber threats autonomously.

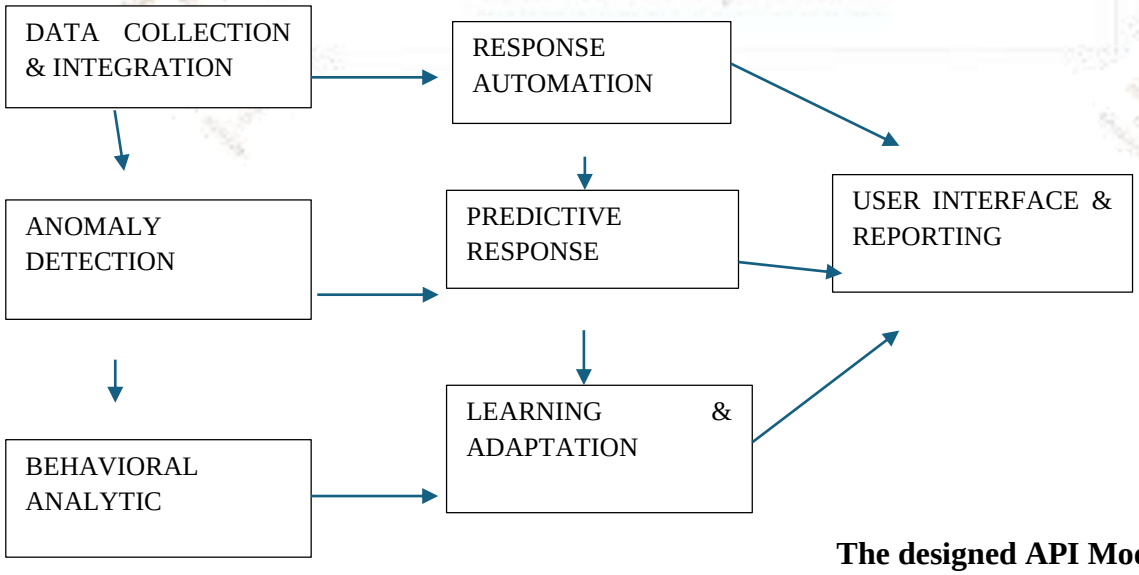
5. Continuous Learning and Adaptation

The continuous learning and adaptation model are very vital for keeping artificial intelligence model effective against the evolving cyber threat. The machine learning algorithms must be regularly updated with new data to adapt to new attack techniques and improve their accuracy. Dilek (2015) highlighted the importance of scalability and adaptability in their artificial intelligence base security framework by ensuring the system remain robust against the emerging cyber threats.

6. Users interface and reporting

The user-friendly interface and reporting are key for an efficient and effective cybersecurity management. These tools provide security analyst with actionable insights and facilitate decision making. The detailed report and dashboards help in understanding the security posture, identifying trends and evaluating the effectiveness of the security measures in place. Li (2018) underscored the significant of a robust user interface in their machine learning system model which aid in monitoring and responding to power grid security incidents effectively.

Figure 1: A designed Pictorial Model for artificial intelligence system in cyber incidents mgt



The designed API Model

Source: Created by the Author

The model figure 1. depicts the pictorial view of artificial intelligence application in the management of cybercrime incidents. The application uses machine learning algorithms multifaceted intelligence agents to demonstrates the capabilities and efficiency in the detection, analysis and prevention of cybercrime incidents on critical infrastructure. Which could be showed in terms of efficiency according to (Sasmal, 2021).

Improved detection

Studies have demonstrated that Artificial intelligence model enhances the detection of cybercrime incidents by employing sophisticated algorithms and machine learning models to identify patterns and anomalies that signify malicious functions. According to Sasmal (2021) machine learning could process and analyze large volumes of data, enables it to detect even subtle signs of fraudulent behavior that traditional method can fail. Artificial intelligence model significantly monitors network traffic, users' behavior and events patterns in real-time, timely alerts and reducing the window of privilege for cyber criminals. The improved detection capabilities of artificial intelligence models have significantly demonstrated the efficiency of multifaced intelligence agents in cybercrime incidents management following various studies such as Lakmali (2024) and Verdoliva (2020) in mitigating threats before any significant harm.

Driving Operational Efficiency

Other studies like Adesuwa, et.al (2019) and Abdiyeva et.al (2021) have shown how Artificial intelligence model drives operational efficiency using automating routine and repetitive tasks to allow cybersecurity specialist to focus more on a complex and high priority issues. Sasmal (2021) study emphasizes the need for artificial intelligence powered tools that can handle task such as data analytics, threat monitoring, and initial incident response thereby significantly reducing the workload of human investigations and long-time checks. The results show significant level of speed and accuracy in threat detection and allow skill professional to concentrate in strategic planning and analyzing on sophisticated attack scenarios by freeing up investigation resources (Becue et.al 2021)

Artificial intelligence Vs Artificial intelligence

Studies have shown the adverse effect of artificial intelligence tools in cybercrime incidents on critical infrastructure. The deployment of artificial intelligence tool Vs AI to counter fight has brought limitation to it efficiency. Sasmal (2021) study show artificial intelligence can counteract Artificial intelligence driven cyber threats by anticipating and neutralizing malicious artificial intelligence algorithms which effectively creates an arm race in the cyber domain. The study further highlighted the importance of the intelligent agents if effectively trained, it can recognize and respond to AI generating phishing emails, malware and other form of cyber-attack incidents. Though the dynamic and adaptative nature gives the algorithms the ability to learn each encounter and continuously improving the defense line against any evolving threats for system efficiency. The proactive approach of the system enables the system stay ahead of sophisticated cyber adversaries.

However, figure 1. Model have been able to demonstrate the significance of artificial intelligence tools to bring efficiency in the fight against cybercrime incidents following some impactful findings by previous and present resaechers like Adesuwa, et.al (2019) and Abdiyeva et.al (2021), Their studies have demonstrated the role of artificial intelligence (AI) in enhancing cybersecurity efficiency despite the limitation and challenges highlighted in the findings**.** Artificial intelligence tool significant effectiveness in automation, pattern recognition, and predictive analysis, detecting and preventing cybercrime incidents.

Other studies such Sasmal (2021), Verdoliva et.al (2020) also agrees with Adesuwa, et.al (2021) and Abdiyev et.al (201) studies on the use of Artificial intelligence-driven models to improve detection capabilities, operational efficiency, and can counteract Artificial intelligence-driven cyber threats, by creating dynamic defense system. However, the findings could not collobrate on the inability of intelligence agents to resolve vulnerabilities reevolving around advanced threats. Though their findings underscores the necessity of Artificial intelligence in modern cybersecurity due to the sophisticated techniques employed by cybercriminals and also the call for improvement on the multifacets intelligence agents for "AI vs. AI," incidents management. Where artificial intelligence agents are used to counteract artificial intelligence-driven cyber threats, creating a kind of arms race in the cyber domain. This development is seen as crucial to proactively stay ahead of sophisticated cyber adversaries.

1.5 EMPIRICAL STUDIES RELATING TO THE THEORETICAL FRAMEWORK OF ARTIFICIAL INTELLIGENCE IN THE PREVENTION OF CYBER FRAUD INCIDENTS

With the increasing prevalence of cybercrime and data beaches incidents among individuals, organizations and national economies risk severe threats from these malicious actors.it is now necessary to take adequate measures to protect the digital space from these malicious threats. The use of artificial intelligence model has become imperative in the art of cybersecurity in our today's business model compared to the traditional approach. A lot of research has been performed on the use of artificial intelligence model in managing cybercrime incidents. Some studies have shown efficiency in the use of artificial intelligent agents in protecting critical assets and the financial sector while others have demonstrated the negative limitation and challenges of the model in terms of false positive and cost compared with the traditional method. This study will examine the contributions of various works in the use of artificial intelligence model in the prevention of cybercrime incidents.

Artificial intelligence started back in 1950s with several years of changes and transformation in the field among various scholars to show a broader relevance of the subject study.

Turning (1950) was the first to discuss "computing machinery and intelligence" in his book in which he presented a methodology for examining machine intelligence. Which is the light for the early stages of artificial intelligence in protecting and enhancing the computer system.

John McCarthy (1956) The father of artificial intelligence who formulated the word "artificial intelligence" elaborated to say the combination of science and engineering to make intelligent device for human welfare will make it more effective for work function. The study went further to itemize the ability of artificial intelligence agents in terms of performance compared to the human brain in making analytic and decision.

According to the author in the findings improved model of machine could do muscle work and illustrate complex questions in an intellectual manner.

Gou et.al (2006) while reviewing previous work in artificial intelligence designed a multi-agent system for detecting computer worm and containment in metropolitan area network which automatically contain propagation of worms that might cause harm to a lot of computer network bandwidth and routers damage. The finding show that the system effectively averts the worm agenda despite the high level of worm infections making the incidents a failed mission.

While Kotenko and Ulanov (2007) evaluated the efficiency of artificial intelligence model in cybercrime incidents proposed a framework for adaptive and cooperative defense mechanism against cybercrime attack. The model uses intelligent multi agent modelling and simulation where groups of intelligent agents interact and adjust configuration and behavior base on the network state and severity of attack. They experiment with a distributed DoS attack and defense mechanism. The findings show cooperation and the ability to adapt to intelligent agent group in making the defense line efficient against any cyber-attack. Though the result has some shortcoming due to the number of sample size for the study to validate the effectiveness but show efficiency in control when compared with the traditional method.

Singh et.al (2011) in another study examines the efficiency of fuzzy network intrusion detection method base using class association rule mining in genetic network programming. The examined model shows flexibility and efficiency for misuse and anomalies to detect network ability to deal with mixed data bases having both discrete and attributes to mining**,** The experiment and measurement of the proposed method show that the technique provides a competitively high detection rates in comparison with other machine learning model when analyze, indicating impactful success in both evaluating discrete and preventing anomalies network. In contrary some of the results indicate false positive when compared other machine learning.

Kumar and Reddy (2014) study evaluate the use of a unique agent base intrusion detection system for wireless network that collect information from various lines and use the information with an evolutionary artificial intelligence system to detect and prevent attack through bypassing and relaying of transmission over the intrusion path. The result show that the system is well suited for attack detection and prevention in wireless network even though the finding indicated some limitation in the use of artificial intelligence in collecting discrete information, given by false positive results.

Gonzalez et.al (2015) went in the same direction as (Gou, et.al 2006) making an improvement in their study using a distributed agent coalition system that preserves normal operations, they implement operational and security strategies that handles unforeseen events and protect against malicious insiders, error and attack in distributed electric grid to see if there could be favorable rate of attack, but the penetration test failed, it show more reliability when compared to the traditional concept and cost.

Dilek et.al (2015) in their study uses uncommon behavior spotting and limitation of looking only for unknown attack pattern in cyber domain. They proposed that the measured variables can be addressed by having a model that engages in continuous learning and re-profiling of standard behavior and use a recognition making command to reduce the false positive. Their study plan is based on process design, inspired by the biological immune model combined with the direct sense making decision to spot and prevent attack in cyber domain.

The findings show high relevance impact in the use of machine learning to evaluate and prevent uncommon behavior, even though the finding show some limitation of false positive results.

Li (2018) researched on the potential of intelligent agent technology for improving operations and response of power grids, preventing malicious actors and reducing their capabilities. They applied multi layered security model prototype that protect against invalid configurations and ability to notice and recover from undisclosed malicious strategies that disrupt the service using the cyberspace. The uncovering shows no penetration success but complete control for detection and prevent of malicious actors.

Collins et.al (2019) in their study a conceptual layered approach for protecting power grid automation system against cybercrime incidents which comes from the internal network sources. One of the components of their framework are security agents, intelligence that could spot infraction occurrence and activities within the controllers. The result obtained by testing a sample of the proposed method show that the system can manage and mitigate some vulnerability issues of power grid automation system, making it more effective against any cyber incidents.

Mohamadou et.al (2020) presented a simple network base infraction spotting and prevention system (IDPS) that uses series of machine learning algorithms to spot and examine network attacks. They used online network environment for the test and the result showed the proposed IDPS offer a higher spotting rate for the main attack type (probe and DoS) in few seconds and automatically protect the computer system from series of attacks and the network.

Chinedu et.al (2021) presented a study of network infraction spotting method based on a genetic algorithm technic with a high population size and operator to optimize the search for attack structure within a realistic processing time. The outcome shows the employed genetic algorithm boost performance and reduced the false positive rate.

Abdiyeva-Alyeva et.al (2021) proposed an artificial intelligence system based on network security situation assessment model that could make real time and quantitative security situation assessment of a network system and provide real time support, and defense measures. The result shows a positive response in real time anomaly detection for network security.

Solomon et.al (2022) study evaluated ways of preventing cyber fraud in the Nigeria Banking system while using a model fraudaeck (fraud analysis environment for cyber fraud) designed with artificial intelligence tool for analyzing identity verification and system authentication to prevent fraud attack. The model uses interconnected subsystem of communication and bank applications. The findings reveal vulnerability in term of software attack such as Xenomorph Trojan to access the banking system making way for imminent cyber-attacks. In conclusion they went further to argue at the end the result show positive outcome for those using electronic banking transaction that the model could detect network attack, identity theft and cyber fraud incidents. However, the findings could not further evidence the prevention in identity theft even though the result show significant impact network detection and other cybercrime incidents.

Gunavathi et.al (2024) proposed a bio-inspired host-based multi-layered intrusion detection system using multiple detection engines and sequential pattern recognition. The result show that the model effectively classifies known behavior and malicious attack. It could auspiciously identify region where irregularities could occur with lower false positive rate compared to other existing strategy. They argued that the model uses intelligent and computational method to spot undisclosed malware and malicious attack in wide-reaching complex network.

Mohammed et.al (2024) investigated the implication of artificial intelligence while using ChatGPT model within the realm of cybersecurity. They use real cutting-edge real scenario of ChatGPT in the field of cybersecurity but illustrate with a case of how ChatGPT could be optimized to formulate false data injection attack against critical assets like industrial control system. They went further to explain how the tool could help security analyst in analyzing, designing and creating security solutions to fight cyber fraud incidents and malicious attack on network. Also, they raised concern for open artificial intelligence privacy policy which outlines the type of data collection required from users and the type to be stored and utilized.

Wang et.al (2024) study focused on improving the performance of intrusion detectors of IDSs. They proposed a hybrid method that uses the searching performance of an immune algorithm to generate a fuzzy detector. The conclusion shows the searching power of immune algorithm, could make fuzzy detection rules minimize the frangibility of detectors and increase detection precision.

Ekekihl (2024) study explore the good and bad of artificial intelligence tools for potential abuse. They focus on the intersection of artificial intelligence and cybersecurity with emphasizes on artificial intelligence generated phishing emails. A mixed method technique was applied with experiment interview and survey using 9 participants from different backgrounds but novices in phishing. In the experiment phishing email were created in distinct three ways, human generated, internet aided, and artificial intelligence created. The mails were examined in a semi structured interview and each participants reviewed 6 emails in total, two of these, were real fishing. The results from interview show that artificial intelligence generated phishing emails are persuasive as those created in human crafted type. On the contrary participants ranked artificial intelligence Phishing as the most persuasive, ranked next to human created, though familiarity play a key role in both persuasiveness and willingness to go along with request phishing emails which was highlighted during the interview and survey. A mixed result was given as potential misuse and negative counteractive using artificial intelligence in the fight against cybercrime incidents.

1.5.1 SUMMARY ANALYSIS AND SYNTHESIS OF THE THEORETICAL FRAMEWORK

Artificial intelligence (AI) has increasingly been employed to strengthen global security framework and prevent cybercrime and fraud incidents. This review complies contributions from several researchers, emphasizing both the effectiveness and limitation associated with applying AI tools to combat cybercrime incidents.

Kotenko and Ulanov (2007) developed an adaptive and cooperative defense mechanism framework to counter cyber fraud. Their model utilizes intelligent multi-agent systems, wherein agents dynamically adjust their configurations and behaviours based on the network state and the severity of attacks. They focused on

investigating defense mechanisms against distributed denial-of-service (DDoS) attacks. Their findings revealed that collaboration and adaptability among intelligent agents significantly improve the effectiveness of defensive measures, underscoring the necessity of intelligent, adaptive responses to evolving cyber threats when compared with the traditional method and cost.

Qiang and Yiqian (2010) introduced an AI-based network security situation assessment model that facilitates real-time, quantitative threat evaluation. This model enhances dynamic defense adjustments, anomaly detection, and situational awareness. The research emphasizes that real-time monitoring and situational awareness are crucial in the rapidly changing cyber threat landscape.

Singh et al. (2011) proposed a novel fuzzy network intrusion detection approach that relies on class association rule mining within genetic network programming. Their system is both flexible and efficient, capable of detecting network misuse and anomalies in mixed databases that include both discrete and continuous attributes. High detection rates in their experiments highlight the superior performance of this method compared to traditional machine learning techniques, providing significant advantages in securing complex, data-rich systems.

Kumar and Reddy (2014) designed an agent-based intrusion detection system for wireless networks. This system collects information from multiple sources and uses evolutionary AI techniques to detect and mitigate attacks, often by rerouting or bypassing transmissions. Their research shows that this system is particularly effective for securing wireless communications, a growing area of concern as wireless networks become increasingly prevalent and vulnerable.

Dilek (2015) introduced a security framework based on artificial immune system principles for mobile ad-hoc networks. This framework emphasizes scalability, robustness, and self-recovery while addressing issues like bandwidth conservation. Drawing from biological immune systems, the model promotes resilience and autonomous recovery, essential features for maintaining robust network security.

Gonzalez et al. (2015) and Li (2018) explored cybersecurity strategies for power grids, a critical infrastructure vulnerable to sophisticated cyberattacks. Gonzalez et al. developed a distributed agent coalition system to ensure the grid's stability while defending against malicious insiders and unforeseen events. Li introduced a multi-layered security model that protects the grid from invalid inputs and detects unknown attack strategies. These studies emphasize layered defense and the strategic use of intelligent agents to secure vital infrastructure.

Collins et al. (2019) advanced these ideas by proposing a theoretical, layered approach for protecting power grid automation systems using intelligent security agents. Their prototype showed significant effectiveness in managing vulnerabilities, reinforcing the necessity of proactive, real-time detection and response mechanisms to counter emerging threats.

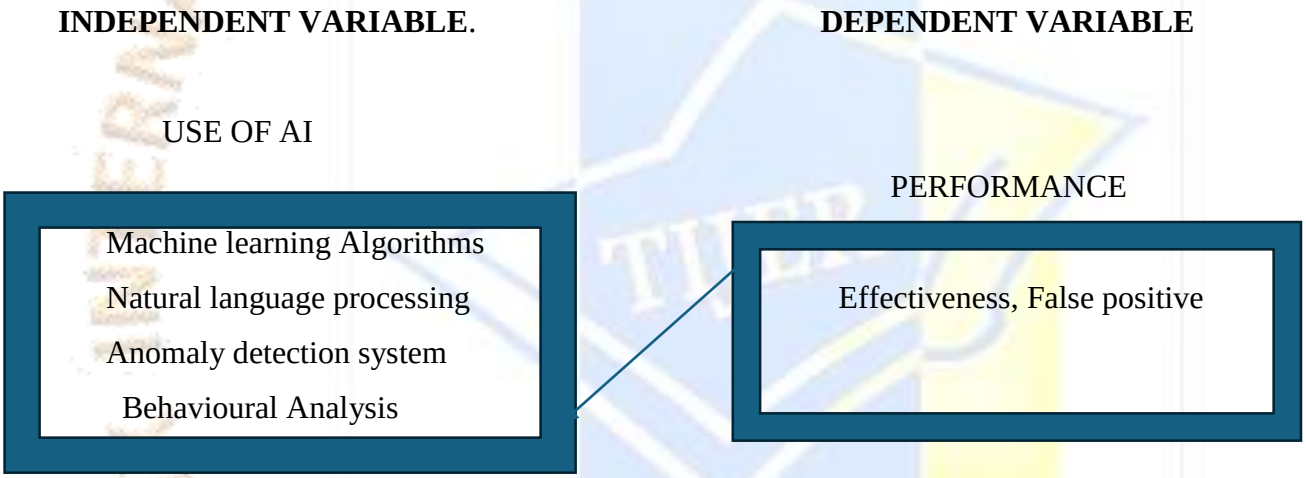
Solomon et al. (2022) and Mohammed et al. (2024) provided a comprehensive historical analysis of AI's development, starting from John McCarthy's foundational work in 1956. They discussed the evolution of machine learning tools and their application in combating cyber fraud. Both authors highlighted the double-edged nature of AI: while it is powerful in detecting cyber threats, it also poses a risk when misused. This

duality becomes increasingly concerning as AI technology advances, making ethical AI development and robust safeguards more crucial than ever.

Ekekihl (2024) focused on the potential for AI misuse in phishing attacks. Through a mixed-method approach involving experiments, interviews, and surveys, Ekekihl demonstrated that AI-generated phishing emails are particularly convincing and effective. This work underscores the necessity of implementing strong measures to defend against AI-powered social engineering attacks.

Marques et al. (2024) presented a mobile intelligent multi-agent system designed to autonomously address Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The system operates using Prolog to function autonomously without human intervention. Their research illustrates the increasing importance of AI-driven, automated threat response systems, which are crucial for combating complex and large-scale cyberattacks.

The model presented (Figure 2) illustrates the relationship between the independent variable, AI application, and the dependent variable, cybersecurity performance. This depiction shows how various AI-based methods as discussed by scholars in their findings influence the effectiveness and limitations of cybersecurity strategies.



Model figure.2. Created by author

The model depicts the performance of AI application in various cybercrime incidents showing the indicative results of various perspectives of scholars in their studies on AI model.

Incidents detection Rate: Studies by Kotenko and Ulanov (2007), Gonzalez et al. (2015), and Li (2018) highlight the critical role of adaptability and cooperative multi-agent systems in responding to dynamic threats. These adaptive strategies are increasingly important as cyberattacks become more sophisticated. The use of Mult-agent systems enables prompt detection of cybercrime incidents using mixed approach of AI model.

Response time to incidents: Qiang and Yiqian (2010) and Collins et al. (2019) emphasize the necessity of real-time monitoring and anomaly detection. Rapid threat detection and response are vital for minimizing damage in a fast-paced cyber landscape using mixed AI model.

Incident Resolution Rate: Contributions by Singh et al. (2011) and Kumar and Reddy (2014) focus on intrusion detection, offering innovative approaches for managing complex data and protecting wireless networks. Their methods demonstrate marked improvements over traditional intrusion detection systems.

Cost of incidents management: Solomon et al. (2022), Mohammed et al. (2024), and Ekekihl (2024) address the paradox of AI in cybersecurity. While AI is an essential tool for threat detection, it also poses significant risks if exploited maliciously. Ekekihl's work emphasizes the ease with which AI can effectively manage cybercrime but was concern about the cost when compared with the traditional method.

False Positive Rate: Marques et al. (2024) offer insights into autonomous AI-driven defense mechanisms that function without human intervention. Their work suggests a promising future for self-operating cybersecurity systems capable of responding to threats with unprecedented speed and scale which might prompt incorrect flags of non-existing cyber incidents.

Overall, while AI holds immense potential to improve cybersecurity performance, it also carries the risk of misuse, as evidenced by various studies. The research underscores the necessity of a balanced approach that maximizes AI's defensive capabilities while mitigating its vulnerabilities. As emphasized by Mohammed et al. (2024) and Ekekihl (2024), ethical development and robust frameworks are paramount to ensure the effective and secure use of AI in combating cybercrime.

1.6 NIGERIAN CYBER FRAUD INCIDENT PREVENTION POLICY MODEL

The rising incidence of cybercrime in the 21st century has necessitated the use of artificial intelligence (AI) tools to safeguard the integrity, confidentiality, and availability of data across critical infrastructure and the financial sector. The significance of robust cybersecurity measures cannot be overstated, as they are vital in defending against various forms of cybercrime. Concerns about cybercrime and fraud continue to impact critical assets and financial institutions. The widespread adoption of digital technology has inadvertently provided opportunities for cybercriminals to exploit and generate income.

Research studies, such as those by Marques et al. (2024) and Ekekihl (2024), have demonstrated the dual impact of AI: while AI enhances cybersecurity efficiency, it is also vulnerable to misuse, facilitating cybercrimes like phishing, malware, identity theft, scams, spoofing, hacking, and DDoS attacks. These incidents have significant implications for critical infrastructure and Nigeria's financial sector, leading to considerable financial losses. For instance, Nigeria reportedly loses up to $400 billion to cybercrime annually and faces a projected risk of $6 trillion in losses by 2030 (Mohammed, 2024). Consequently, Nigeria has undertaken a review and redesign of its cybersecurity framework, incorporating AI as a strategic tool for crime prevention and mitigation, guided by the Budapest Convention of 2001.

Despite the introduction of AI tools for cybersecurity, many public and private organizations in Nigeria have yet to fully implement these technologies to protect critical infrastructure, with the notable exception of the financial and national defense sectors. Some industries have adopted machine learning tools partially, mainly due to the high costs associated with comprehensive AI solutions.

In response to persistent vulnerabilities caused by human error and the escalating threats from cybercriminals, President Olusegun Obasanjo's administration established several enforcement agencies. This action was prompted by ongoing pressure from the Financial Action Task Force (FATF), highlighting Nigeria's non-

compliance with international standards on combating cybercrime and fraud. Through parliamentary acts, agencies such as the Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and Other Related Offenses Commission (ICPC), State Security Services (SSS), and the Nigerian Police were created to combat and enforce laws against cybercrime. This study will examine the impact of these agencies in the use of AI in preventing and mitigating cybercrime incidents in Nigeria critical assets and financial sector.

1.6.1 THE ECONOMIC AND FINANCIAL CRIME COMMISSION (EFCC)

The Government of President Olusegun Obasanjo established the institution in 2003, it was created in response to the pressure from international organization such as (FATF) Financial Action Task Force. Due to Nigeria noncompliance with global standard for the prevention of cybercrime and fraud incidents. The institution is mandated to conduct investigations related to cybercrime and fraud incidents and other related offenses. The evidence acts are revised in 2011 to allow for admission of electronic evidence in 2015 for an effective criminal justice procedure due to lack of legal framework for cybercrimes. The cybercrimes (Prohibition, Prevention and Punishment) act of 2015 establishes a single and all-embracing legal, regulatory framework for Nigeria in the prohibition, detection, enforcement and punishment of cybercrimes offenders. The Nigerian Government in February 2015 welcome the creation of the National cybersecurity policy and strategy which was produced by the inter-ministerial committee and managed by the office of the national security adviser because of Nigeria involvement in the Budapest 2001 convention. It is based on the advice of 2001 Budapest convention, that Nigeria executed and adopted threats to information and critical technology infrastructure as a danger to the national security that could affect economic, political and social fabric. Cybercrimes, cyber espionage, cyber conflicts, cyber terrorism, child internet abuse, cyber fraud incidents and exploitation were among some of the set down as the most serious concerns. The objective is to handle cybersecurity risks following the overarching national security goals. However, the policy has been very successful following the increasing Nigeria cyber resilience with the use of artificial intelligence tools (Adesuwa et.al (2019). The agencies promote and protects critical information technology infrastructures, cybersecurity, computer network and system, electronic communication, data and computer program and privacy rights. They perform investigation and prosecute cases for cybercrimes and other related cybersecurity offenses.

1.6.2 NIGERIAN COMPUTER EMERGENCY RESPONSE TEAM (NG-CERT)

According to OAL (2021) the Nigerian cybercrime act 2015 was passed to support cybercrimes prevention and cybersecurity by requiring the private and public sector such as ISPs, telecommunication operators and financial institutions to report incidents and cooperate with law enforcement agencies and Nigerian computer emergency response team (Ng-Cert). The Cybercrime advisory council help to facilitate the effective implementation of cybersecurity policy, capacity building, multi-stakeholder engagement, inter-agency and international cooperation with national security advisor, also coordinating LEAs and the attorney general of federation office by overseeing, strengthening the legal and institutional framework of the Nigerian cybersecurity.

The Nigeria National Security Adviser administers the national cybersecurity measures. Other key supporting agents are government agencies and private sector businesses. In terms of the overall cybersecurity strategy, the Nigerian government offers strategic guidance. The objective of the Nigerian CERT is to administer the risks of cyber threat in Nigeria's cyberspace and efficiently coordinate incidents response and mitigate plans to proactively prevent cyber-attack incidents in Nigeria. The office of the National security adviser stipulates the following as the functions and primary objectives of Nigerian-CERT.

1. Formulate a common situation awareness platform to coordinate information sharing on national scale.
2. Properly handle and coordinate the management of national interest incidents
3. Aid in the implementation of national cybersecurity policy
4. Give technical assistance and knowledge to sectorial CSIRT as needed to function as the worldwide point of contact for all cyber security incidents in Nigeria.

1.6.3 THE NIGERIA CYBERCRIME ADVISORY COUNCIL

The cybercrime advisory council is established in March 2016 by articles 42 and 43 of the cybercrime act. The members consist of ministries and agencies of governments that are supervised and directed by the national security adviser. They are created to attend to the growing threat of cybercrime in Nigeria due to the increasing rise of the digital technology. The cybercrimes act of 2015 was introduced to address this problem by the creation of legal and regulatory model for the prevention, investigation and prosecution of cybercrime. The council is responsible for the implementation of the act by guiding the government on issues relating to cybersecurity and cybercrimes. The task is to provide guidance on the development and execution of strategies that would prevent cybercrimes, protect critical assets and ensure safety and security of Nigeria cyberspace. The members consist of the following

1. National security Adviser (NSA) Chairperson of the council sadden with the responsibility for coordinating the Nigeria national cybersecurity functions.
2. Representatives from different Government agencies and ministries: These involves the members of the ministry of Justice, communication, Ministry of defense, Central Bank of Nigeria, Telecommunication, Nigeria police and others sister agencies.
3. Private sector groups: This members from the private sectors mostly those from the critical industries like Banking, telecommunication, Power and energy and information technology. This group provide insights and expertise from their respective sectors and contributing to the development of a holistic cybersecurity policies.

The responsibilities of the councils include:

1. Advising on cybersecurity policies and strategies: The council is saddle with the function for advising the government on the formulation and implementation of a national cybersecurity policies, strategies and programs. They include providing recommendation on the protection of national critical assets and how to manage an emerging cyber threat.

2. Coordinating and collaboration with different stakeholders involved in cybersecurity such as government agencies, private sector group and international partners through the promotion of cooperation and unity for a better model to combating cybercrime.
3. Monitoring and Reporting: The council is given the responsibility to monitor the implementation of cybersecurity policies and strategies as well as the examining the effectiveness. The council report its findings to the government and make recommendations for the improvement where necessary.
4. Capacity building and public awareness: The council work to promote capacity building and awareness on cybersecurity as it relates to Nigeria through training program for enforcement officers, agencies and creating public awareness through campaigns, flyers and other initiatives aimed at protecting the overall cybersecurity and critical infrastructure assets.
5. Advising on legal and Regulatory matters: The councils provide guidance on the development and amendment of laws and regulations related to cybersecurity and
6. cybercrime. This ensures that the Nigeria's legal framework remains updated and effective in addressing the evolving nature of cyber threat to critical infrastructure and assets.

1.7 THE NIGERIAN FINANCIAL SECTOR CYBERSECURITY LANDSCAPE

According to the International Monetary Fund's (IMF) Financial Stability Report (2024), the global financial system remains highly vulnerable to cybercrime and fraud incidents due to its handling of sensitive data and information. Research has shown that cybersecurity threats pose significant risks to the Nigerian financial sector and national assets, jeopardizing the confidentiality, integrity, and availability of financial services and data. Attacks involving malware, Distributed Denial of Service (DDoS), and injection threats are particularly concerning, as they can severely disrupt the financial system and compromise critical infrastructure. However, the integration of artificial intelligence (AI) has significantly enhanced the ability of the financial sector to protect against and prevent these cyber threats.

The Nigerian financial sector plays a crucial role in the nation's economy, serving as a foundation for economic transactions and wealth management. Yet, it is consistently under threat from various cybersecurity risks that threaten its stability and integrity. Understanding these threats is vital for developing effective countermeasures to safeguard Nigeria's financial systems and critical infrastructure. This research draws on past and current studies to examine the use of AI in managing cybersecurity incidents, providing insight into Nigeria's cybersecurity policy landscape.

One of the most significant threats to Nigeria's financial sector is malware, which encompasses a wide array of malicious software designed to infiltrate computer systems, disrupt operations, and steal sensitive data (Furnell and Warren, 2003). The application of AI has proven crucial in addressing these vulnerabilities, as AI-driven solutions can detect and prevent sophisticated cyber threats more efficiently. Additionally, Distributed Denial of Service (DDoS) attacks are a major challenge, exploiting human error and overwhelming servers with traffic to make services unavailable to customers (Hovav, 2003). Studies have demonstrated that the financial sector and national critical infrastructure, such as the PowerGrid and banking services, are

frequent targets of DDoS and other cyberattacks. Research by Ekekihl (2024) highlights the effectiveness of AI in mitigating these threats, although some studies have noted issues with false positive results.

AI tools have been shown to significantly curb cybercrime in the Nigerian financial sector by leveraging machine learning to manage and prevent fraud incidents. AI's ability to provide sophisticated analysis and countermeasures against evolving cyberattacks is a key innovation. It can analyse patterns, monitor cyber hazards, and proactively address potential incidents (Nweke and Yayilgan, 2024). Some AI systems are designed to learn and adapt without human intervention, making decisions autonomously and replicating human problem-solving processes to streamline operations (Emmanuel et al., 2023).

The development and implementation of AI-driven models for cybersecurity in Nigeria's financial sector and critical infrastructure have been widely embraced. Machine learning algorithms and deep learning models are used to detect, assess, and respond to cyber threats with high speed and accuracy, as noted in studies by Ekekihl (2024) and Adesuwa and David (2019). The integration of AI has revolutionized cybersecurity, enabling automated systems to protect financial transactions and national assets effectively (Reis et al., 2024).

Extensive research continues to address AI-related challenges in identifying threats such as deepfakes and other complex cybercrimes. The Nigerian financial sector is increasingly prioritizing cyber-risk management to protect financial integrity and customer assets, as emphasized by Adesuwa and David (2019). The sector remains a prime target for advanced and persistent threats (Garba et al., 2022). Nevertheless, AI has made a substantial impact, enhancing data mining, forensic analysis, and digital investigations to manage cybercrime and safeguard critical assets effectively.

1.8 NIGERIA CYBERSECURITY MODEL

Cyber fraud incidents are a significant component of cybercrime that pose serious threats to Nigeria, especially given the country's increasing reliance on digital platforms for economic, political, and social activities. Cybercrime impacts not only the privacy, integrity, and accessibility of computer systems and data but also undermines the foundational values and long-term stability of societies that depend on digital technology. Key challenges to Nigeria's national security include cybercrime, cyber-espionage, cyber-conflict, cyber-terrorism, and child online abuse and exploitation.

Given these threats, the Nigerian government cannot afford to be passive. It must actively defend critical infrastructure against cybercrime. Although vast amounts of cybercrime occur daily on digital platforms worldwide, only a small fraction of perpetrators are prosecuted. Nigeria's cybersecurity model is structured to prevent and combat cybercrime through a blend of strategies developed from academic research and international conventions.

The Nigerian cybersecurity framework draws from various international guidelines, including the African Union Convention on Cyber Security and Personal Data Protection, adopted in Malabo in June 2014. This treaty underscores a commitment among African Union member states to establish a secure and trustworthy information society (Dasuki, 2014). The framework covers areas such as electronic transactions, personal data protection, and the handling of cybersecurity and cybercrime incidents. However, the model remains relatively

unproven and less robust compared to frameworks in more developed nations, such as the Budapest Convention of 2001.

The Budapest Convention, supported by the Cybercrime Convention Committee and capacity-building programs, provided a foundation for Nigeria's legal framework against cybercrime. According to Mohammed (2020), Nigeria's Cybercrime Act of 2015 was a key step in building an effective cybersecurity system. The country's cybersecurity strategies focus on protecting critical infrastructure and investing in capacity building, with researchers evaluating the effectiveness of these efforts.

Adesuwa et al. (2019) emphasizes the importance of public awareness and education to prevent cybercrime and fraud. They advocate incorporating cybersecurity education into school curricula and conducting nationwide awareness campaigns to inform the public about cybercrime risks and prevention methods. The goal is to reduce the success rate of cybercriminals by equipping the population with knowledge to avoid falling victim to phishing, social engineering, and other fraudulent schemes.

Similarly, Garba (2022) supports the call for strengthening critical infrastructure, capacity building, and local expertise. This model encourages substantial investment in cybersecurity education and training to develop a skilled workforce capable of managing critical assets and responding to emerging threats. It also promotes the use of technology, such as firewalls, intrusion detection systems, and encryption, to reduce vulnerabilities to cybercrime.

Sidik et al. (2020) highlight the importance of public-private sector partnerships to protect critical assets. They argue for collaboration through information sharing, joint training, and coordinated response strategies. These partnerships enhance Nigeria's ability to detect and mitigate cybercrime by involving national security agencies in enforcement actions to trace and freeze fraudulent activities.

Sabillon (2022) stresses the need for a comprehensive legal framework to manage cybercrime and fraud. This includes revising existing laws, enforcing strict penalties, and improving the judicial system to handle cybercrime cases efficiently. Stronger legal measures would deter cybercriminals and facilitate international cooperation for tracking and prosecuting cross-border cybercrime, which is a significant issue in Nigeria.

Overall, Nigeria’s evolving cybersecurity model incorporates elements from both local and international best practices. It encompasses critical infrastructure development, a robust legal framework, public awareness, and public-private partnerships. Despite challenges like limited funding and a weak legal system, these strategies lay a solid foundation for improving Nigeria's cybersecurity landscape. By adopting and adapting international best practices, Nigeria can build a resilient cybersecurity system to protect its citizens and critical infrastructure from various forms of cyber-attacks.

1.8.1 NIGERIA CYBERSECURITY MODEL IN RELATION TO OTHER COUNTRIES

Nigeria’s cybersecurity framework is relatively underdeveloped compared to those of more advanced nations. It is influenced by a combination of local research, legislative efforts, and international guidelines, including those of the European Union, the Budapest Convention of 2001, the African Union, and ECOWAS. The main objective of Nigeria’s model aligns with global efforts to protect and prevent critical infrastructure from being increasingly targeted by cybercriminals.

Many studies have examined Nigeria's cybersecurity strategies in comparison with other nations. For example, Lebogang et al. (2022) analysed national cybersecurity models across Africa, highlighting Nigeria's framework as part of a larger continental plan to secure cyberspace. Similarly, Ikuero (2022) discussed the establishment of key institutions such as the Nigeria National Computer Emergency Response Team (CERT), Sectoral Computer Security Incident Response Teams (CSIRTs), and the National Cybersecurity Policy and Strategy (NCPS) under the Office of the National Security Adviser (ONSA), all aimed at strengthening the nation's cybersecurity coordination.

However, research by Ikuero and Zeng (2022) has pointed out several weaknesses in Nigeria's cybersecurity policies. While comprehensive in some areas, these policies fail to address certain critical aspects of cybersecurity effectively. According to Damilola et al. (2023), the model also lacks initiatives to raise public awareness about cybersecurity, such as integrating mandatory cybersecurity courses into school curricula a practice common in more developed countries (Othman, 2022). The international comparison of Nigeria's cybersecurity strategies reveals a need for unifying national security measures and adjusting them to meet global standards.

Sabillon (2022) notes that the European Union's approach prioritizes cross-border cooperation, regulatory frameworks, and harmonization of cybersecurity practices among member states. By contrast, Nigeria's strategy remains more internationally focused than nationally driven. Adopting a more nationalistic approach with an emphasis on regulatory harmonization and localized implementation could strengthen Nigeria's cybersecurity framework rather than relying heavily on European models and framework.

The Nigerian cybersecurity landscape is crucial for the protection of the financial sector and critical infrastructure. Its exposure to a wide range of cyber threats, including malware, Distributed Denial of Service (DDoS) attacks, and other worm-based intrusions, is a significant concern for both stakeholders and researchers. These threats jeopardize the stability and integrity of financial systems, often resulting in substantial financial losses and data breaches. However, there has been a growing interest in incorporating artificial intelligence (AI) into Nigeria's cybersecurity framework, marking a significant advancement for the financial sector and critical infrastructure. Studies have demonstrated the effectiveness of AI models, such as machine learning and deep learning algorithms, as essential tools for detecting, evaluating, and mitigating cyber threats with enhanced speed and precision.

Research by Adesuwa et al. (2019), Garba et al. (2022), Ekekihl (2024), and others has highlighted the efficiency of AI tools in combating cybercrime and fraud incidents, despite some limitations, such as false positive outcomes. Although AI models, particularly those based on machine learning and deep learning, offer promising prospects for protecting and managing critical assets, the effectiveness of these tools is not without challenges. Some studies emphasize their success, while others point to limitations.

This study will analyse the theoretical framework and methodology to assess the effectiveness of artificial intelligence in managing cybercrime within critical infrastructure and the financial sector. The findings will be presented and analysed to determine the empirical impact of AI applications in cybercrime incidents.

2.0 THE THEORETICAL FRAMEWORK OF THE RESEARCH METHODOLOGY IN THE USE OF ARTIFICAL INTELLIGENCE IN PREVENTION OF CYBERCRIME & FRAUD INCIDENTS IN THE NIGERIA FINANCIAL SECTOR AND NATIONAL CRITICAL ASSETS.

Cybercrime is an attack not just on the privacy, validity, accessibility of computer data and system but on the underlying values and long-term prospects of societies that are increasingly reliant on the digital technology. This chapter aims to examine the application of artificial intelligence (AI) in combating cybercrime and fraud incidents. The methodology outlined here will guide in the systematic presentation, collection, analysis, and interpretation of data to assess the impact of artificial intelligence-based solutions in cybersecurity. The methodology outlined will provide a structured approach to analysis of the use of Artificial intelligence in combating cybercrime and fraud incidents in Nigeria financial sector and critical asset. The findings will contribute to a deeper understanding of how artificial intelligence application could enhance cybersecurity efforts and inform the development of a more effective strategies to protect the financial sector and national critical assets from being a cyber-attack incident. How effective will artificial intelligence application be in the fight against cyber-crime and fraud incidents in Nigeria financial sector and national critical Assets.

2.1 RESEARCH DESIGN

The study will employ a quantitative research design. The design can provide meaningful insights into the research question. It gives a comprehensive understanding of how artificial intelligence technologies are applied in cybersecurity and their impact on preventing cybercrime and fraud incidents in the Nigeria financial sector and critical assets. A case studies of organizations that have successfully implemented Artificial intelligence applications in their cybersecurity strategies will be examined. The case study design is chosen in this study because it gives the researcher in-depth knowledge and information about the participants in the study. It is unbiased, efficacy, reliable, and valid in the outcome. These case studies shall provide in-depth insights into:

- The implementation process of AI technologies.
- Quantitative and qualitative outcomes achieved.
- Lessons learned and best practices.

The study shall use statistical method to analyse the quantitative data collected from surveys and case studies. Techniques such as descriptive statistics, regression analysis, and correlation analysis shall be used to:

- Measure the relationship between Artificial intelligence application adoption and reduction in cybercrime incidents.
- Assess the effectiveness of Artificial intelligence tools in various contexts (e.g. sector, organization size).
- Identify patterns and trends in the use of Artificial intelligence for cybersecurity.

Other studies such as Montasari and Hill (2019), Des and Sandhane (2021), and Meraj et.al (2022) justify the use of quantitative methods using descriptive statistics in their study analysis outcome and analysis of secondary statistical data and presentation.

However, the motivated for this research is my desire to contribute to this area of research that has been untapped in Nigeria in the use of artificial intelligence in the management of cybercrime incidents in Nigeria due to the increase in cybercrime activities perpetuated by Nigerian across the globe. The research problem has continued to linger for a decade, and researcher are still having nightmare. I have agreed to explore this avenue to make an impact in this academic loophole and bridge the gap on empirical works in Nigeria. Furthermore, it is also part of the requirements for academic qualification.

RESEARCH AIM AND OBJECT OF RESEARCH

The research object – The use of artificial intelligence to manage cybercrime incidents.

The aim of the study is to examine the use of artificial intelligence in manging cybercrime incidents in Nigeria critical assets and the financial sector.

2.2 THE RESEARCH OBJECTIVES

The following research objectives shall be achieved in the study:

1. To assess the effectiveness of Artificial intelligence applications in managing cybercrime incidents in Nigeria financial sector and critical assets.
2. To identify the major type of cybercrime incidents in the Nigeria critical assets and the financial sector.
3. To evaluate the impact of Artificial intelligence-based cybersecurity measures on the overall security posture and incident response times within Nigeria critical assets and the financial sector.
4. To analyse the type of artificial intelligence technologies currently being utilized in mitigating cybersecurity incidents in Nigeria critical assets and the financial sector.

2.3 RESEARCH QUESTION AND FORMULATION OF HYPOTHESIS

The study will formulate some research questions and hypothesis to measure the variables in the theoretical model in the use of artificial intelligence tools to manage cybercrime incidents in the Nigeria critical assets and the financial sector. The following research questions and hypothesis are designed to pursue the research aim and objectives:

Research Objective 1: To identify the types of Artificial intelligence technologies currently being utilized in cybersecurity for combating cybercrime.

Research Question 1:

What are the specific Artificial intelligence technologies being deployed in cybersecurity to combat cybercrime?

Hypothesis 1:

The most used Artificial intelligence technologies in cybersecurity include machine learning algorithms, natural language processing, behavioural analysis, and predictive analytics.

Research Objective 2: To assess the effectiveness of Artificial intelligence applications in reducing the incidence of cybercrime in the Nigeria financial sector and critical assets.

Research Question 2:

How effective are Artificial intelligence applications in reducing the incidence of cybercrime in Nigeria' critical assets and the financial sector?

Hypothesis 2:

Artificial intelligence applications significantly reduce the incidence of cybercrime in Nigeria's critical assets and financial sector compared to traditional cybersecurity measures.

Research Objective 3: To explore the limitations associated with the use of Artificial intelligence in cybersecurity practices in quick response to detection of cybercrime**.**

Research Question 3:

What are the key limitations encountered in the use of Artificial intelligence in cybersecurity practices*?*

Hypothesis 3:

AI in cybersecurity is significant a high costs, complexity and efficiency when compared with traditional model.

Research Objective 4: To evaluate the impact of Artificial intelligence-based cybersecurity measures on the overall security posture and incident response times within organizations.

Research Question 4:

What is the impact of Artificial intelligence-based cybersecurity measures on the overall security posture and incident response times within organizations*?*

Hypothesis 4:

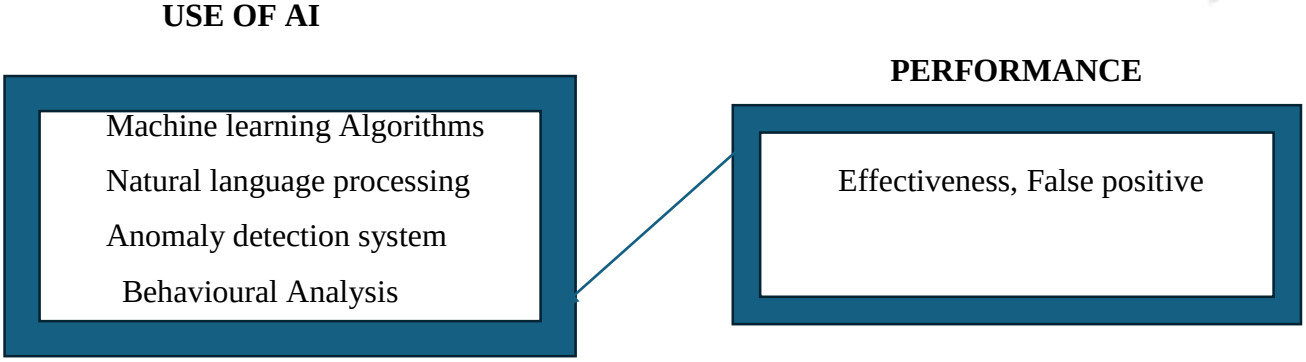
Organizations that implement Artificial intelligence-based cybersecurity measures experience a significant improvement in their overall security posture and a reduction in incident response times.

These research questions and hypotheses are designed to guide the study towards achieving its objectives by focusing on specific aspects of Artificial intelligence application in cybersecurity. Each hypothesis is formulated to be tested through empirical data analysis, aligning with the quantitative and qualitative research strategy to test the object of research.

2.4 RESEARCH MODEL

The theoretical model of the research shows the relationship between the variable for measurement.

INDEPENDENT VARIABLE. **DEPENDENT VARIABLE**



Model figure.1. Created by author

The theoretical model illustrates the relationship between our independent and dependent variables, highlighting the performance of AI models in managing cybercrime incidents within Nigeria critical assets and the financial sector. The performance will be assessed based the following variables.

1. **Incident detection rate:** Research by Kotenko and Ulanov (2007), Gonzalez et.al (2015) and Li (2018) among others, underscores the vital role of artificial intelligence model in incident detection. This study will evaluate the effectiveness of AI model in detecting cybercrime within Nigeria's critical assets and the financial sector.
2. **Response time to incidents**: Qiang and Yiqian (2010) and Collins et.al (2019) highlight the importance of real time monitoring and anomaly detection. Quick threat detection and response are essential for minimizing damage in the evolving cyber landscape, particularly when utilizing the mixed method of AI models. The use of these application will help this study determine the effect in terms of response to anomaly detection.
3. Incidents Resolution rate: Contributions from Singh et.al (2011) and Kumar and Reddy (2014) focus on intrusion detection and present innovative strategies in managing complex data incidents. This variable will assess AI model ability to facilitate rapid detection and resolutions of incidents when it occurs.
4. Cost of incident management: Solomon et.al (2020), Mohammed et.al (2024) explore the paradox of AI in cybersecurity. This variable will compare the cost associated with AI driven incidents management and resolution against the traditional method.
5. False positive rate: Insights from Marques et.al (2024) discuss autonomous AI driven defense mechanisms that operate with human intervention. Their findings suggest a promising future for self-operating cybersecurity system capable of responding to threat with remarkable speed and scale, although this may lead to incorrect flags for non-existent cybercrime incidents.

However, while AI model has significant potential to enhance cybersecurity performance, the variables outlined will be measured to evaluate the effectiveness of AI model in managing cybercrime incidents within Nigeria's critical assets and the financial sector, ultimately determining their efficiency in combating cybercrime in the empirical data presentation and analysis.

2.5 RESEARCH DATA COLLECTION

The study will primarily rely on primary statistical data, sourced from the study sample size, with questionnaires distributed among specialist in Nigeria's critical assets and financial sector using Artificial intelligence tools in managing cybercrime incidents. The survey will aim to capture the perspectives of respondents on the effectiveness of Artificial intelligence applications in preventing cybercrime, the limitation, and the perceived impact on their operations. This is performed using google-online survey to reach out to the proposed sample size taking into consideration the population estimated margin of error in the study.

2.6 RESEARCH QUESTIONNAIRE DESIGN

The questionnaire will consist of both closed-ended and open-ended questions. Closed-ended questions will use a Likert scale to measure the level of agreement or disagreement with statements related to Artificial intelligence's effectiveness in cybercrime prevention. Open-ended questions will allow respondents to provide more detailed insights and suggestions. Participants will be selected using a purposive sampling method to ensure that those who are directly involved in cybersecurity and fraud prevention activities within financial institutions are included in the study. Prior, to data collection, consent will be obtained from the academic supervisor overseeing the research and senior management within the participating financial institutions. This step ensures the ethical integrity of the research and the validity of the measured variables.

2.7 DATA ANALYSIS

Descriptive statistical techniques will be employed to analyse the collected data. This will involve summarizing and interpreting the data to assess performance and identify correlations in the use of Artificial Intelligence (AI) applications within Nigeria's financial sector, as well as their role in managing cybercrime incidents. SPSS software will be used for data analysis, based on completed and submitted questionnaires related to the study.

Inferential statistical methods will also be applied to draw conclusions from the data that can be generalized to the wider population. Techniques such as chi-square analysis and standard deviation will be used in hypothesis testing to assess the significance of the relationship between AI implementation and its effectiveness in addressing cybercrime incidents in Nigeria's financial sector, with a focus on critical assets.

Standard Deviation: To examine the variation in the use of AI models in relation to the frequency of cybercrime incidents.

Chi-Square Analysis: To evaluate the impact of AI applications on preventing cybercrime incidents and identify which specific AI techniques are most effective.

2.8 THE SAMPLING AND SELECTION OF RESPONDENT

Our research sample size will be 500, consisting of employees working in both the private and the public sector, in-charge of information technology and critical asset management in Nigeria. To determine the appropriate sample size for a population of 500 individuals in the context of assessing the use of artificial intelligence (AI) in managing cybercrime incidents in Nigeria critical assets and the financial sector, we utilize a statistical method with a 95% confidence level and a margin of error·

Key Parameters:

Population Size (N): 500 (the total population of potential respondents)

Confidence Level: 95% (the probability that the sample accurately reflects the population within the margin of error)

Margin of Error (E): Typically set at 5% (0.05), this indicates the degree of allowable error in the results

Proportion (P): 0.5, assuming maximum variability since no prior data exists

Sample Size Formula:

The following formula is used to calculate the sample size for finite populations:

n = \frac {{N \cdot Z^2 \cdot P \cdot (1-P)}}{{E^2 \cdot (N - 1) + Z^2 \cdot P \cdot (1 - P)}}

Where:

- n =Sample size
- N = Population size (500)
- Z = Z-value (1.96 for a 95% confidence level)
- P = Estimated proportion of the population (assumed to be 0.5)
- E = Margin of error (0.05 for 5%)

Calculation Steps:

1. Calculate the Z-score:

Z = 1.96 \quad \text {(for 95% confidence)}

2. Calculate the proportion P:

P = 0.5 \quad \text {(assuming maximum variability)}

3. Set the margin of error E:

E = 0.05 \quad \text {(5% margin of error)}

4. Substitute values into the formula:

n = \frac {{500 \cdot (1.96) ^2 \cdot 0.5 \cdot (1 - 0.5)}} {{(0.05) ^2 \cdot (500 - 1) + (1.96) ^2 \cdot 0.5 \cdot (1 - 0.5)}}

5. Calculate the sample size:

Using the formula, the calculated sample size is approximately 218 to determine the margin of error to validate, the reliability of the study.

Interpretation:

For a population of 500 individuals with a 95% confidence level and a 5% margin of error, the calculated sample size required to accurately represent the population is 218 respondents. This ensures that the results of the research will reflect the views and experiences of the population with a high degree of accuracy.

This sample size will provide reliable insights into the use of AI in managing cybercrime incidents in Nigeria' critical assets and the financial sector, ensuring that the results are generalizable to the broader population.

2.8 RESEARCH LIMITATION

The study in the use of artificial intelligence application in managing of cybercrime incidents in Nigeria's critical assets and the financial sector faces several significant limitations due to few sectors that has fully implemented using artificial intelligence tools in the fight against cybercrime in Nigeria's critical assets. The study faces data constraints, and technological gaps. Addressing these limitations could be critical in enhancing research reliability for ensuring that Artificial technologies can be effectively deployed in combating cybercrime and protecting critical assets within the Nigerian financial system·

3.0 EMPRICIAL DATA PRESENTATION, ANALYSIS, AND FINDING

This chapter presents the results of the data analysis, the interpretation of the results, and a discussion of the findings. The data collected for this study were primarily collected by administering a questionnaire to the Nigeria's critical assets and the financial sectors

3.1 DESCRIPTIVE ANALYSIS OF DEMOGRAPHIC INFORMATION OF RESPONDENTS

This section presents the analyses of the number of questionnaires distributed, returned, usable, and non-usable for the study. In addition, in this section, the demographic information of the respondents was analysed using Google Forms.

3.1.1 DESCRIPTIVE ANALYSIS OF THE ADMINISTERED RESEARCH INSTRUMENTS

TABLE 3.1.1: RESPONSE RATE

Description	***Frequency***	***%***
Copies of the questionnaire filled	178	81.7
Copies of the questionnaire not filled	40	18.3
Total Copies of Questionnaire Administered	**218**	**100**

Source: Field Survey (2024)

Table 3.1 shows the response rate of the respondents on the distributed questionnaire. The table shows that two hundred and eighteen (218) copies of the questionnaire was the targeted responses but one hundred and seventy-eight (178) were properly filled, and used for the analysis of this study. This represents an 81.7% response rate.

3.1.2 DESCRIPTIVE ANALYSIS OF DEMOGRAPHIC INFORMATION OF THE RESPONDENTS

THIS SECTION PRESENTS THE DEMOGRAPHIC INFORMATION OF THE RESPONDENTS

TABLE 3.2: DESCRIPTIVE STATISTICS OF RESPONDENTS' DEMOGRAPHIC INFORMATION

		Frequency	Percentage (%)
Gender	Male	117	65.7
	Female	64	34.3
Age	18-25	26	14.6
	26-35 years	47	26.4
	36-45 years	62	34.8
	46-55 years	28	15.7
	56years and above	15	8.4
Educational Qualification	Diploma	9	5.1
	Bachelor's Degree	99	55.6
	Master's Degree	51	28.7
	Doctorate	14	7.9
	Others	5	2.8
Job Role	IT Manager	26	14.6
	Security Analyst	4	2.2
	Compliance Officer	22	12.4
	Cybersecurity Specialist	20	11.2
	Others	106	59.6
Work Experience	Less than 1 years	16	9.0
	1-3 years	53	29.8
	4-6 years	47	26.4
	7-10 years	10	5.6
	Over 10 years	52	29.2
Organization	Commercial Bank	20	11.2
	Insurance companies	5	2.8
	(FinTech) Company	22	12.4
	Government Agency	34	19.1
	Others	97	54.5%

Source: Researcher's computation (2024).

Table 3.2 provides detailed descriptive statistics of respondents' demographic information, which sheds light on the diversity and composition of the study participants across various characteristics. The analysis begins with gender distribution, which indicates that most respondents (117 individuals, 65.7%) were male, while females constituted 64 (34.3%) of the sample. This skewed distribution suggests a higher representation of male participants in the study.

The age distribution of respondents reflects a varied demographic profile, with the highest number of participants aged 36-45 years, accounting for 62 individuals (34.8%). This is followed by those in the 26-35 years age group, comprising 47 respondents (26.4%). Participants aged 46-55 years number 28 (15.7%), while the youngest age group, 18-25 years, included 26 individuals (14.6%). Finally, 15 respondents (8.4%) were aged 56 years. These figures illustrate that most respondents fall within the middle-age range (26-45 years), potentially indicating a workforce with moderate to substantial professional experience.

The educational qualifications of respondents varied significantly, with 99 individuals (55.6%) holding a bachelor's degree. Respondents with a master's degree followed, totaling 51 (28.7%), while those with a doctoral degree numbered 14 (7.9%). Only nine respondents (5.1%) had a diploma, and five (2.8%) reported

having other qualifications. These data point to a well-educated sample, with a predominant focus on higher education levels that are likely indicative of specialized skills in their respective roles.

In terms of job roles, the majority, 106 respondents (59.6%), fall under the 'Others' category, suggesting a wide range of positions not specified in the primary list. IT Managers comprised 26 individuals (14.6%), while Compliance Officers accounted for 22 individuals (12.4%). Cybersecurity Specialists numbered 20 (11.2%), and Security Analysts represented the smallest portion, with only 4 respondents (2.2%). This distribution highlights the study's focus on a broad range of roles related to IT, cybersecurity, and compliance.

Work experience among respondents was diverse, with 53 individuals (29.8%) having 1-3 years of experience, forming the largest group. Respondents had over 10 years of experience follow closely, totaling 52 (29.2%). The 4-6 years of experience group included 47 respondents (26.4%), while those with less than one year of experience numbered 16 (9.0%). Only ten respondents (5.6%) had 7-10 years of experience. The data suggest a significant representation of individuals with varying levels of professional exposure from entry-level to highly experienced.

Finally, the organizational distribution of respondents indicates that the majority, 97 individuals (54.5%), are employed in unspecified 'Other' organizations. Government agencies accounted for 34 respondents (19.1%), while Fintech companies included 22 respondents (12.4%). Commercial banks employed 20 individuals (11.2%), and insurance companies had the smallest representation, with five respondents (2.8%). This range demonstrates a diverse mix of participants from different sectors, emphasizing the relevance of this study across multiple industries, especially in sectors tied to financial services and government operations.

3.2 DESCRIPTIVE STATISTICS OF RESEARCH HYPOTHESIS ONE

HYPOTHESIS ONE: TO IDENTIFY THE TYPES OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES CURRENTLY BEING UTILIZED IN CYBERSECURITY FOR COMBATING CYBERCRIME

Table 2: Types of AI Technologies currently utilized in cybersecurity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Machine Learning Algorithms	16	9.0	9.0	9.0
	Natural Language Processing	27	15.2	15.2	24.2
	Predictive Analytics	60	33.7	33.7	57.9
	Automated Threat Detection Systems	17	9.6	9.6	67.4
	Behavioral Analysis Tools	58	32.6	32.6	100.0
	Total	**178**	**100.0**	**100.0**	

Source: Researcher's computation (2024).

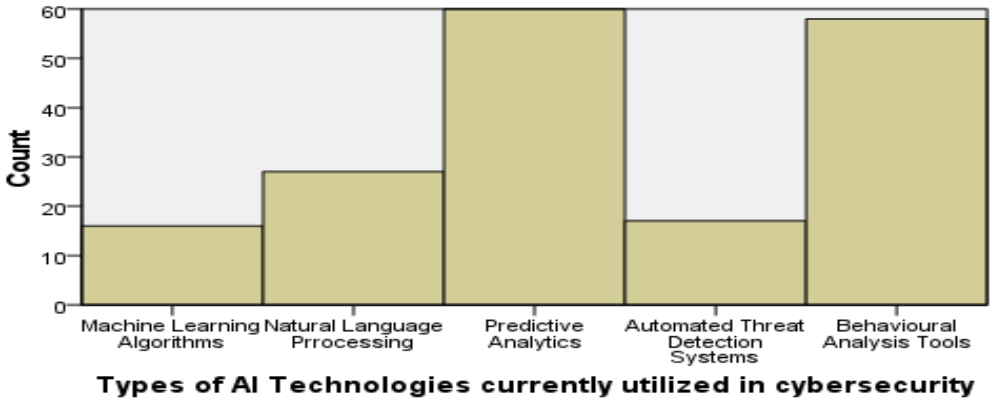


Table 2. Provides a clear breakdown of the types of artificial intelligence (AI) technology currently being utilized in cybersecurity to combat cybercrime incidents.

The total sample size for the analysis was 178 each type for AI technology listed has a corresponding frequency, percentage, validity percentage and cumulative percentage to illustrate its prevalence in current cybersecurity practices.

The most frequently mentioned AI technology was predictive analytics which accounted for 60 respondents, making up 33.7 % of the total. This high percentage indicates that predictive analytics is a leading cybersecurity technology, favoring its ability to forecast potential threats based on historical data patterns and trends. Its dominant presence suggests that cybersecurity professionals value their proactive approach in detecting and preventing cybercrime incidents.

Behavioral analysis tools used by 58 respondents, representing 32.6% of the total sample. These tools analyses users' behavior and detect anomalies that can indicate malicious activities. The nearly equal prevalence of predictive analytics and behavioral analysis tools suggests that these two technologies are widely recognized as effective in identifying potential threats through pattern recognition and anomaly detection.

Natural language processing (NLP) was the next most commonly uses technology with 27 respondents (15.2%) Natural processing language is particularly useful for analysis communication and extracting actional insights that could reveal phishing attempts or malicious intent in emails and text-based messages. Its moderate usage highlights, its specialized role in cybersecurity, complementing other AI tools with a focus on language text analysis.

Automated threat detection system was used by 17 respondents, accounting for 9.6% of the sample. These systems automate the process of identifying potential security threats in real time and offer quick response capabilities. While not as frequently used as others top technologies, automated threat detection is essential for enhancing the speed and efficiency of cybersecurity operations.

Finally, machine learning algorithms was used by 16 respondent 9.0%. machine learning is fundamental to many AI-based security tools, enabling system to learn from the data and improve their performance over time. However, its frequency is lower than that of other technologies, machine learning is often integrated into

more complex systems, including predictive analytics and automated threats detection to enhance its capabilities.

In summary the data indicate that predictive analytics and behavioral analytics tools are the most utilized AI technologies in cybersecurity, collectively making up over 66% of the respondents. The ability of these tools to anticipate and analyze behavior makes them highly effective in combating cybercrime incidents. Although technologies such as Natural language

processing, automated threat detection anomaly system and Machine learning algorithms also play significant roles, their adaptation rates are comparatively lower, suggesting more specialized or supporting functions in the broader cybersecurity landscape.

3.3 Descriptive Statistics of Research Hypothesis Two

Table 3: To assess the effectiveness of Artificial intelligence applications in reducing the incidence of cybercrime in the Nigeria financial sector and critical assets

Item	SA	A	N	D	SD	Mean	Skewness	Kurtosis
My organization effectively uses AI technologies to combat cybercrime	37 20.8%	81 45.5%	47 26.4%	9 5.1%	4 2.2%	2.22	0.671	0.567
AI application have reduced the frequency of cyber fraud incidents in my organization	37 20.8%	91 51.1%	45 25.3%	5 2.8%	0 0.0%	2.10	0.234	-0.337

Source: Researcher's computation (2024).

Table 3 provides insights into respondents' perceptions of the effectiveness of AI applications in reducing cybercrime within Nigeria's financial sector and critical assets. For the statement, "My organization effectively uses AI technologies to combat cybercrime", 66.3% of respondents either strongly agreed or agreed, showing a generally positive perception supported by a mean score of 2.22. A skewness value of 0.671 indicates a moderate concentration of responses on the positive side, suggesting a slight majority consensus, although 26.4% remained neutral. A kurtosis of 0.567 implies that the responses are more spread out than normally distributed, highlighting some variability in opinions.

Regarding the statement, "AI applications have reduced the frequency of cyber fraud incidents in my organization", 71.9% of respondents strongly agreed or agreed, reflected by a mean of 2.10. The distribution of responses is relatively balanced with a slight positive skewness (0.234), indicating that opinions leaned towards agreement but with some neutrality (25.3%). The kurtosis of -0.337 suggests that responses are moderately spread, showing a broader range of views, but still indicating a positive trend. Overall, these findings point to a general belief in the positive impact of AI in combating cybercrime, with room for some respondents to be further convinced of its effectiveness.

Hypothesis Two:

Does Artificial application effectively reduce the incidence of cybercrime within Nigeria critical assets and the financial sector compared to the traditional method?

Test Statistics

AI_technology_currently_utilized_in_cybersecurity	
Chi-Square	86.742[a]
Df	6
Asymp. Sig.	0.000

0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 25.4.

The chi-square test results indicated a significant association between the use of AI technology in cybersecurity and its effectiveness in reducing incidents of cybercrime within the critical assets and the financial sector. With a chi-square value of 86.742 and 6 degrees of freedom, the P-value was .000 (P<0.001), confirming a strong statistical significance. This suggest that the observed data significantly differs from what would be expected under the null hypothesis, indicating that AI applications are indeed effective in reducing cybercrime. Additionally, with no cells having expected frequencies less than 5, the test's reliability was confirmed.

3.4 Descriptive Statistics of Research Hypothesis Three

TABLE 4: TO EXPLORE THE LIMITATIONS ASSOCIATED IN THE USE OF ARTIFICIAL INTELLIGENCE IN MANAGING CYBER INCIDENTS

Item	SA	A	N	D	SD	Mean	Skewness	Kurtosis
To what extent do you agree with the following statement: "using AI in cybersecurity presents significant limitation	46	85	46	4	0	2.06	0.197	-0.582
	24.2%	47.8%	25.8%	2.2%	0.0%			
AI-based systems have impacted to a significant reduction & financial loss within Nigeria's critical assets and financial sector.	37	90	40	11	0	2.14	0.433	-0.186
	20.8%	50.6%	22.5%	6.2%	0.0%			

Source: Researcher's computation (2024).

The data in Table 4 reflect responses regarding the limitation and impact of implementing AI in cybersecurity practices. For the statement, "Implementing AI in cybersecurity presents significant limitation", 47.8% of respondents agreed and 24.2% strongly agreed, indicating that a majority (over 70%) acknowledged the presence of notable limitation in adopting AI for cybersecurity. The mean response of 2.06, combined with a slight positive skewness (0.197) and negative kurtosis (-0.582), suggests that most responses leaned toward agreement with some variation, but the overall distribution was slightly spread out with fewer extreme values. For the statement, "AI-based systems have contributed to a significant reduction in financial losses due to cybercrime within Nigeria's critical assets and the financial sector", 50.6% of respondents agreed, and 20.8% strongly agreed, indicating that the majority (around 71%) recognized AI's positive impact in reducing financial losses. The mean response of 2.14 supports this positive perception. A skewness of 0.433 suggests a moderate rightward skew, indicating that more responses leaned toward agreement. A kurtosis of -0.186 implies a distribution that is flatter than normal, showing a moderate spread in the agreement levels. Overall, these responses highlight both the recognized limitation and the perceived impact of AI in cybersecurity.

Hypothesis Three: Does implementation of AI model in cybersecurity has limitations in cybercrime incidents.

Test Statistics

Cybersecurity challenges	
Chi-Square	160.292[a]
Df	5
Asymp. Sig.	0.000

a. 0 cells (0.0%) have expected frequencies less than
5. The minimum expected cell frequency is 29.7.

The Chi-Square test results indicated a significant association between the implementation of AI in cybersecurity and the limitations encountered. A Chi-Square value of 160.292 with five degrees of freedom and an asymptotic significance (p-value) of 0.000 ($p < 0.001$) strongly suggests that these challenges are significant and not due to random chance.

The fact that no cells had expected frequencies less than five, with a minimum expected cell frequency of 29.7, confirms that the test results are reliable. This indicates that organisations that implement AI in cybersecurity are likely to face notable challenges or limitations.

3.5 **DESCRIPTIVE STATISTICS OF RESEARCH HYPOTHESIS FOUR**

TABLE 5: EVALUATION OF THE IMPACT OF ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY MEASURES ON THE OVERALL SECURITY POSTURE AND INCIDENT RESPONSE TIMES WITHIN CRITICAL ASSETS AND THE FINANCIAL SECTOR.

Item	SA	A	N	D	SD	Mean	Skewness	Kurtosis
AI-based cybersecurity measures have improved the overall security posture of Nigeria's critical assets and the financial sector	54 30.3%	80 44.9%	34 19.1%	10 5.6%	0 0.0%	2.00	0.557	-0.280
The implementation of AI in cybersecurity has reduced incident response times within Nigeria's critical assets and the financial sector	32 18.0%	105 59.0%	35 19.7%	6 3.4%	0 0.0%	2.08	0.446	0.352
AI-based systems have contributed to a significant reduction & financial loss within Nigeria's critical assets and the financial sector	34 19.1%	91 51.1%	42 23.6%	11 6.2%	0 0.0%	2.17	0.404	-0.179
How would you rate the impact of AI on the speed of incident response within Nigeria's critical assets and the financial sector	38 21.3%	100 56.2%	39 21.9%	1 0.6%	0 0.0%	2.02	0.091	-0.466
Implementing AI in cybersecurity presents significant limitation	19 10.7%	92 51.7%	48 27.0%	19 10.7%	0 0.0%	2.38	0.405	-0.289
AI-based systems have contributed to a significant quick detection of cybercrime incident within Nigeria's critical assets and the financial sector compared to traditional approach.	31 17.4%	90 50.6%	38 21.3%	18 10.1%	1 0.6%	2.26	0.562	-0.059
AI-based cybersecurity measures have improved the overall security posture of within Nigeria's critical assets and the financial sector	36 20.2%	90 50.6%	45 25.3%	7 3.9%	0 0.0%	2.13	0.290	-0.280
The implementation of AI in cybersecurity has reduced incident response times in within Nigeria's critical assets and the financial sector	27 15.2%	85 47.8%	39 21.9%	23 12.9%	4 2.2%	2.39	0.606	-0.098

AI-based systems have contributed to a significant reduction and financial losses within Nigeria's critical assets and the financial sector	32 18.0%	91 51.1%	45 25.3%	5 2.8%	5 2.8%	2.21	0.873	1.434
How would you rate the impact of AI on the speed of incident response within Nigeria's critical assets and the financial sector	38 21.3%	100 56.2%	39 21.9%	1 0.6%	0 0.0%	2.02	0.091	-0.466

Source: Researcher's computation (2024).

The survey results provide a detailed analysis of the impact of AI-based cybersecurity measures within Nigeria's critical assets and the financial sector security posture and incident response times. A substantial portion of respondents indicated that these measures have significantly improved their overall security, with 30.3% strongly agreeing and 44.9% agreeing that "AI-based cybersecurity measures have improved the overall security posture within Nigeria's critical assets and the financial sector", leading to a mean score of 2.00. A skewness of 0.557 indicates a moderate rightward tendency, suggesting that most respondents leaned toward agreement. Meanwhile, the kurtosis of -0.280 points to a flatter distribution, reflecting some variability in how strongly individuals feel about the improvements, indicating that while many perceive benefits, there are differing levels of conviction among the respondents.

When evaluating the impact on incident response times, the results remained consistently positive. For the statement "The implementation of AI in cybersecurity has reduced incident response times in my organization", 18.0% strongly agreed and 59.0% agreed, resulting in a mean score of 2.08. This finding reinforces the notion that respondents believe that AI technologies enable faster responses to cyber incidents. The skewness of 0.446 suggests a slight rightward skew, indicating that most participants favored this view, while the kurtosis of 0.352 indicated a more peaked distribution, suggesting a stronger clustering of responses around the mean. This highlights a shared belief among organizations within Nigeria's critical assets and the financial sector regarding the effectiveness of AI in improving incident response times.

Furthermore, the impact of AI on financial losses due to cybercrime is notable. The statement "AI-based systems have contributed to a significant reduction in financial losses in organization' within Nigeria's critical assets and the financial sector received responses that led to a mean score of 2.17, with 17.4% strongly agreeing and 50.6% agreeing. A skewness of 0.404 reflects a tendency toward agreement, while a negative kurtosis of -0.179 indicates some variability in the responses. This suggests that, while many organizations are experiencing reduced financial losses due to AI implementation, the extent of these benefits may vary depending on specific circumstances or operational contexts.

Despite the acknowledged benefits of AI, the respondents also highlighted the limitation associated with its implementation. For the statement, "Implementing AI in cybersecurity presents significant limitation", 10.7% strongly agreed and 51.7% agreed, resulting in a mean score of 2.38. A skewness of 0.405 indicates a slight

rightward lean toward agreement, while a kurtosis of -0.289 suggests a flatter distribution of responses. This complexity illustrates that while organizations recognize the advantages of AI, they also face significant hurdles such as increase amount of false positive and lack of expertise when integrating AI technologies into their cybersecurity frameworks.

In summary, the survey results revealed a nuanced landscape regarding AI's role of AI in enhancing cybersecurity within organizations. While the frequency data show a consensus on the positive impacts of AI on security posture and incident response times, the mean scores, skewness, and kurtosis highlight varying degrees of belief and experience among respondents. The presence of challenges underscores the multifaceted nature of implementing AI technologies, suggesting that organizations must navigate these obstacles to fully realize AI's potential benefits of AI. This insight emphasizes the need for ongoing support, training, and strategic planning to effectively integrate AI into cybersecurity practices and to achieve optimal results.

Hypothesis Four: Is there any impact of AI-based cybersecurity measures on the overall security posture and incident response times within organisations?

Test Statistics

Cybersecurity measures	
Chi-Square	53.169[a]
Df	17
Asymp. Sig.	0.000

a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 9.9.

The test statistics indicate a significant relationship between AI-based cybersecurity measures and their impact on the overall security posture and incident response times in organisations within Nigeria's critical assets and the financial sector. A Chi-Square value of 53.169 with 17 degrees of freedom yielded an asymptotic significance (p-value) of .000. This p-value is far below the conventional threshold of 0.05, suggesting that the null hypothesis, asserting that there is no impact of AI-based cybersecurity measures on security posture and incident response times, can be confidently rejected. The results indicate meaningful differences in perceptions or outcomes related to AI implementation in cybersecurity across the sample population.

Moreover, the absence of cells with expected frequencies less than five, along with a minimum expected cell frequency of 9.9, strengthens the reliability of these results. This finding suggests that the sample size and distribution of responses provide a solid basis for generalising the findings. Overall, these statistics imply that organisations within Nigeria's critical assets and the financial sector leveraging AI in their cybersecurity strategies are likely to experience an enhanced security posture and improved incident response times,

confirming the positive influence of AI technologies in safeguarding organizational assets against cyber threats.

3.6 Discussion of Findings

The findings of this study highlight the increasing significance of artificial intelligence (AI) in enhancing cybersecurity measures in organizations within Nigeria's critical assets and the financial sector. Respondents indicated that AI technologies positively influenced the overall security posture, with a significant portion affirming improvements in incident response times. This aligns with the recent literature suggesting that AI can provide predictive analytics, threat detection, and automated responses that outpace traditional cybersecurity measures (Sarkar et al., 2022). The mean responses reflected a favorable perception of AI's role in combating cyber threats, emphasizing its potential to minimize financial losses associated with cybercrime, corroborating the findings of Zhuang et al. (2023), who noted AI's capacity to significantly mitigate risks and losses in the digital landscape.

However, this study also revealed that the implementation of AI in cybersecurity is accompanied by notable limitation. A considerable number of participants acknowledged difficulties in integrating AI technologies into existing cybersecurity frameworks, reflecting sentiments found in the literature where the authors have discussed the complexities of technology adoption (Li et al., 2023). The mean response related to the limitation posed by AI integration was higher than expected, indicating a potential gap in the infrastructure, increase numbers of false positive flags, and skills required for effective implementation. This suggests that while organizations within Nigeria's critical assets and the financial sector recognize the benefits of AI, there remains a significant hurdle in terms of readiness and ability to fully leverage these technologies in the increase rate of false positive outcome.

The frequency of respondents identifying AI technologies, such as predictive analytics and behavioral analysis tools, as essential tools further highlight the trend towards sophisticated cybersecurity solutions. Predictive analytics has been shown to enhance threat detection capabilities, allowing organizations to preemptively address vulnerabilities before they can be exploited (Sharma et al., 2022). The literature supports the notion that leveraging AI for behavioral analysis can lead to improved identification of anomalous patterns indicative of cyber threats, suggesting that organizations could benefit from investing in these specific technologies to bolster their defenses (Chen et al., 2023).

Additionally, the findings indicate that organizations with a higher proportion of personnel experienced in AI and cybersecurity tend to report better outcomes in terms of security posture and incident response. This observation aligns with the research by Chen and Chang (2023), which emphasizes the importance of skilled personnel in successfully deploying AI solutions in cybersecurity. The need for ongoing training and development to keep pace with rapidly evolving cyber threats is evident, reinforcing the idea that organizations must invest not only in technology but also in their human capital to maximize the potential of AI in cybersecurity. AI presents promising advancements in combating cyber threats, in organizations within Nigeria's critical assets and the financial sector must address the associated limitations identified in this study.

It is crucial for organizations to develop clear strategies for integration, invest in training their workforce, and regularly assess the effectiveness of AI technologies in their cybersecurity efforts. By doing so, organizations within Nigeria's critical assets and the financial sector can enhance their security posture and incident response capabilities, ultimately leading to a more resilient defense against cybercrime. Future research could explore the longitudinal impact of AI implementation on organizational security outcomes, thus providing deeper insights into the evolving relationship between technology and cybersecurity practices.

3.6 SUMMARY

Analysis of the respondents' biodata revealed significant demographic diversity within the sample population. Most of the respondents were male (65.7%), compared to female respondents (34.3%). Age distribution showed a balanced representation across various age groups, with the highest percentage (34.8%) falling within the 36-45 years category, followed by the 26-35 years age group (26.4%). This demographic representation indicates that the sample includes a substantial number of individuals who are likely to possess relevant experience and knowledge of cybersecurity practices. The educational qualifications of the respondents highlighted a predominance of bachelor's degree holders (55.6%), followed by master's degree holders (28.7%). Their varied educational backgrounds suggest a wide range of perspectives and expertise in the application of artificial intelligence (AI) in cybersecurity.

The job roles of the respondents reflect a diverse range of positions within organizations, with a notable majority (59.6%) categorized as "Others", which likely includes various roles not specifically identified in the survey. The prevalence of roles such as IT managers (14.6%) and cybersecurity specialists (11.2%) among the respondents indicated a focus on professionals directly engaged in cybersecurity measures. The distribution of work experience shows a balanced spread, with most respondents having between 1-3 years (29.8%) and over 10 years (29.2%) of experience. This diversity in work experience enhances the reliability of findings regarding the impact of AI technologies on cybersecurity practices.

In examining the types of AI technologies currently utilized in cybersecurity, the findings highlight that predictive analytics (33.7%) and behavioral analysis tools (32.6%) are the most widely adopted technologies among respondents. This indicates a trend towards using advanced analytical capabilities to detect anomalies and predict potential cyber threats. Additionally, natural language processing (15.2%) and machine learning algorithms (9.0%) were utilized, suggesting a multifaceted approach to combat cybercrime. The adoption of these technologies underscores the critical role of AI in enhancing the effectiveness of cybersecurity measures within organizations.

Regarding the effectiveness of AI applications in reducing the incidence of cybercrime, the data indicated a generally positive perception among respondents. A mean score of 2.22 reflects that most participants agree that their organizations effectively utilize AI technologies to combat cybercrime. Furthermore, the application of AI was perceived to have contributed to a reduction in the frequency of cyber fraud incidents, with a mean score of 2.10. While the overall sentiment is favorable, the skewness and kurtosis values suggest moderate

agreement levels and some variability in responses, indicating that, while many organizations see benefits from AI, there may be inconsistencies in implementation and effectiveness.

The survey also highlighted the significant challenges associated with implementing AI in cybersecurity practices. With a mean score of 2.06 for the statement regarding the challenges of implementing AI, the findings suggest that a considerable proportion of respondents (approximately 72%) acknowledge that these implementations are fraught with difficulties. This is further corroborated by the chi-square analysis, which shows a significant value (160.292), indicating that challenges exist in adopting AI technologies. The respondents noted issues ranging from resource limitations to the complexity of integrating AI systems with existing cybersecurity frameworks, which may hinder their effectiveness.

Finally, the evaluation of AI-based cybersecurity measures on the overall security posture and incident response times within organizations indicated a strong positive impact, as reflected in a chi-square value of 53.169, with a significance level of 0.000. This finding demonstrates that organizations implementing AI in their cybersecurity strategies experience improved security postures and reduced incident response times. Respondents generally agreed that AI measures contributed to significant reductions in financial losses due to cybercrime, with a notable mean score of 2.21. These findings collectively affirm the critical importance of AI in enhancing organizational cybersecurity while also acknowledging the challenges that arise with its implementation.

3.7 Conclusion

This study underscores the significant impact of artificial intelligence (AI) in enhancing cybersecurity measures within the financial sector in Nigeria. The demographic analysis of the respondents illustrates a diverse and knowledgeable group, predominantly consisting of professionals with substantial educational qualifications and varied experience in cybersecurity. This diverse representation lends credibility to the findings, suggesting that shared perspectives reflect a wide range of experiences with AI technology. The results indicate that organizations are increasingly leveraging AI solutions, such as predictive analytics and behavioral analysis tools, to effectively combat cybercrime.

The effectiveness of AI applications in reducing cybercrime incidents was evident from the positive sentiments expressed by respondents. The mean scores indicated general agreement among participants regarding the successful implementation of AI technologies in their organizations. This finding highlights the perceived benefits of AI, particularly in mitigating cybercrime and improving overall security posture. Furthermore, the data suggest that organizations utilizing AI have experienced reduced incident response times, allowing them to address threats promptly and efficiently. This responsiveness is crucial in today's rapidly evolving cybersecurity landscape, in which the frequency and sophistication of cyber threats are constantly increasing.

Despite the positive impacts of AI on cybersecurity, this study also revealed notable challenges associated with its implementation. Respondents acknowledged the complexities and resource limitations that organizations face when integrating AI systems into existing cybersecurity frameworks and the increase of

false positive flags on detection. These challenges underscore the need for comprehensive strategies to address the potential obstacles to AI adoption. By identifying these barriers, the financial sector can create an environment conducive to successful AI integration, ultimately enhancing their cybersecurity capabilities.

In summary, the findings of this study highlight the dual nature of AI in cybersecurity—its potential to significantly improve security measures, while also presenting limitation that need to be addressed. As the financial sector continue to navigate the complexities of cyber threats, the integration of AI technologies will be essential for strengthening their defenses. Future research should explore strategies to overcome the identified limitation and further investigate the evolving role of AI in enhancing cybersecurity, ensuring that the financial sector and within Nigeria critical sector remain resilient in the face of an ever-changing threat landscape.

3.8 RECOMMENDATIONS

Based on these findings, the following recommendations are made:

i. Organisations within Nigeria's critical assets and the financial sector should prioritise training programs aimed at upgrading the cybersecurity workforce using AI technologies. Given the complexities involved in implementing AI solutions, a well-trained team can effectively navigate these challenges. Continuous professional development workshops and certification courses should be provided to ensure that employees are proficient in the latest AI tools and methodologies to enhance their ability to combat evolving cyber threats.

ii. Organisations within Nigeria's critical assets and the financial sector should develop comprehensive integration strategies that align AI initiatives with existing cybersecurity frameworks to address the limitation associated with the increase numbers of false positive flagging in cyber incidents. This includes conducting thorough assessments of current cybersecurity practices, identifying gaps, and formulating clear plans for integrating AI tools that complement and enhance the existing measures. Stakeholders across different departments should be involved in the planning process to ensure a holistic cybersecurity approach.

iii. Organisations within Nigeria's critical assets and the financial sector should foster a culture that encourages collaboration among IT, cybersecurity, and other departments involved in incident response and security management. By promoting cross-functional teams and open communication, organisations can leverage diverse perspectives to identify potential vulnerabilities and develop innovative AI solutions. Encouraging experimentation and the iterative development of AI technologies will enable organisations to stay ahead of cyber threats and adapt to changing security landscapes.

iv. Organisations within Nigeria's critical assets and the financial sector should implement routine assessment and audit frameworks to evaluate the effectiveness of their AI-driven cybersecurity measures. Regular

v. reviews will help to identify any shortcomings in AI applications and ensure that they meet the organisation's security objectives. These assessments should focus on performance metrics, incident response times, and overall security posture, enabling organisations to make informed decisions on necessary adjustments or enhancements to their AI strategies. Additionally, feedback from employees using these systems can provide valuable insights into their effectiveness and areas of improvement.

LIST OF REFERENCES

1. Alan, M. (1950). Turing. Computing machinery and intelligence. Mind, 59(236), 433-460.
2. Abdiyeva-Aliyeva, G., Hematyar, M., & Bakan, S. (2021, October). Development of System for Detection and Prevention of Cyber Attacks Using Artificial Intelligence Methods. In 2021 2nd Global Conference for Advancement in Technology (GCAT) (pp. 1-5). IEEE.
3. Adeola Oyinlade (2024) An Overview of Cybercrimes and Internet Regulations in Nigeria
4. Adesuwa, E., & David, M.S. (2019). Cyber Crime and Its Economic Impact in Nigeria. Southeastern Journal of Research and Sustainable Development (Sejrsd), 2(1), 16-31
5. Afolayan, A., Plant, E., White, G., Jones, P., & Beynon-Davies, P. (2015, September 1). Information Technology Usage in SMEs in a Developing Economy. Wiley, 24(5), 483-498. https://doi.org/10.1002/jsc.2023
6. Andrei, F., & Veltri, G. A. (2024). Social influence in the darknet market: The impact of product descriptions on cocaine sales. International Journal of Drug Policy, 124, 104328.
7. Bécue, A., Praça, I. & Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Artif Intell Rev 54, 3849–3886 (2021). https://doi.org/10.1007/s10462-020-09942-2
8. Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.
9. Brody, R. G., Kern, S., & Ogunade, K. (2022). An insider's look at the rise of Nigerian 419 scams. *Journal of Financial Crime*, *29*(1), 202-214
10. Canali, D., Bilge, L., & Balzarotti, D. (2014, June). On the effectiveness of risk prediction based on users browsing behavior. In *Proceedings of the 9th ACM symposium on Information, computer and communications security* (pp. 171-182).
11. Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. Review of International Geographical Education Online, 11(7).
12. Collins, G. S., & Moons, K. G. (2019). Reporting of artificial intelligence prediction models. The Lancet, 393(10181), 1577-1579
13. Daniel, et al., (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 7 May 2018
14. Damilola, O., Emmanuel, A., & Ngoc, P.B. (2023). Cybercrime on social media in Nigeria: trends, scams, vulnerabilities and prevention. https://dx.doi.org/10.22624/aims/csean-smart2023p17
15. Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cybercrimes: A review. arXiv preprint arXiv:1502.03552
16. Gautam, A. (2023). The Evaluating the Impact of Artificial Intelligence on Risk Management and Fraud Detection in the Banking Sector. *AI, IoT and the Fourth Industrial Revolution Review*, *13*(11), 9–18. Retrieved from https://scicadence.com/index.php/AI-IoT-REVIEW/article/view/25

17. Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems*, *28*(2), 203-236.
18. Ekekihl, E (2024). Getting the public to create phishing emails: A study on the persuasiveness of AI-generated phishing email vs human methods.
19. Furnell, S. (2023, June). Cybercrime: vandalizing the information society. In international conference on web engineering (pp 8-16) Berlin, Heidelberg: Springer Berlin Heidelberg.
20. Garbarino, S, & Holland,J. (2009) Quantitative and qualitative methods in impact evaluation and measuring results.
21. Garba, A.A., Siraj, M.M., & Othman, S.H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International journal of electricity and computer Engineering (IJECE), 12(1) 572-584
22. Ghazi-Tehrani, A.K, & Ponell, H.N. (2022) Phishing evolves: Analysing the enduring cybercrime. In the new technology of financial crime (pp.35-61). Routledge
23. Ghazi M Qasaimeh, & Hussam Eddin Jaradeh. (2022). The impact of artificial intelligence on the effective applying of Cyber governance in Jordanian Commercial Bank. International Journal of Technology, Innovation and Management (IJTIM), 2(1). https://doi.org/10.54489/ijtim.v2i1.61
24. Gao, Y., Miao, H., Chen, J., Song, B., Hu, X., & Wang, W. (2022). Explosive cyber security threats during covid-19 pandemic and a novel tree-based broad learning system to overcome. *IEEE Transactions on Intelligent Transportation Systems*, *25*(1), 786-795.
25. Gumbi, D. (2018). Understanding the threat of cybercrime: A comparative study of cybercrime and ICT legislative framework of South Africa, Kenya, India, the United States and United Kingdom
26. Gunavathi, R., & Bharathi, K.M (2024) 2 Cybercrimes in the. Artificial intelligence for cyber defense and smart policing, 21
27. Haenlein, M., Kaplan, A., Tan, C. W., & Zhang, P. (2019). Artificial intelligence (AI) and management analytics. Journal of Management Analytics, 6(4), 341-343.
28. Hernandez-Castro, J., & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. Computer Fraud & Security, 2014(2), 5-8.
29. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189
30. Kaya, O., Schildbach, J., AG, DB, & Schneider, S. (2019). Artificial intelligence in banking. Artificial intelligence
31. Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar (2022) Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, Cybernetics and Systems, DOI: 10.1080/01969722.2022.2112539
32. Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. In Autonomous Intelligent Systems: Multi-Agents and Data Mining: Second International Workshop, AIS-ADM 2007, St. Petersburg, Russia, June 3-5, 2007
33. Hovav, A., & D'Arcy, J., 2003. The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review, 6(2), 97-121
34. Ikuero, F.E., & Zeng, W. (2022). Improving cybersecurity incidents reporting in Nigeria: micro and small enterprises perspectives. Nigerian Journal of Technology, 41(3), 512-520. https://dx.doi.org/10.51594/csitrj.v5i2.761
35. Jain, M., Sinha, A., Agrawal, A., & Yadav, N. (2022, November). Cyber security: Current threats, challenges, and prevention methods. In *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)* (pp. 1-9). IEEE.
36. Kaya, O., Schildbach, J., AG, DB, & Schneider, S. (2019). Artificial intelligence in banking. Artificial intelligence

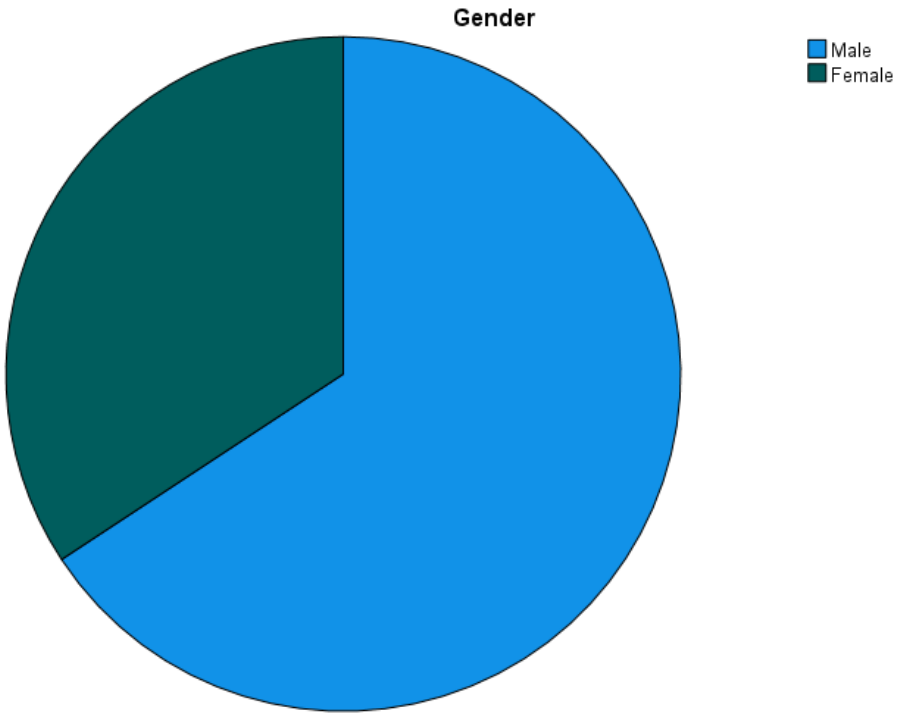
37. Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar (2022) Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, Cybernetics and Systems, DOI: 10.1080/01969722.2022.211253
38. Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. In Autonomous Intelligent Systems: Multi-Agents and Data Mining: Second International Workshop, AIS-ADM 2007, St. Petersburg, Russia, June 3-5, 2007
39. Lakhchini, W., Wahabi, R., El Kabbouri, M., Bp, C., & Hassan, S. (2022). Artificial Intelligence & Machine Learning in Finance: A literature review. International Journal of Accounting, Finance, Auditing, Management and Economics
40. Laas, O. (2023). Deepfakes and trust in technology. Syntheses, 202(5), 132.
41. Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating cybersecurity strategies in Africa. In Cybersecurity capabilities in developing nations and its impact on global security (pp. 1-19). IGI Global. https://dx.doi.org/10.4018/978-1-7998-8693-8.ch001
42. Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.
43. Mabunda, S. (2017, May). Applying the Gordon & Ford categorisation and the routine activities theory to cybercrime: A suitable target. In 2017 IST-Africa Week Conference (IST-Africa) (pp. 1-10). IEEE.
44. Marques, P., Pádua, L., Sousa, J. J., & Fernandes-Silva, A. (2024). Advancements in Remote Sensing Imagery Applications for Precision Management in Olive Growing: A Systematic Review. Remote Sensing, 16(8), 1324.
45. Mavridis, C. N., Kanellopoulos, A., Vamvoudakis, K. G., Baras, J. S., & Johansson, K. H. (2023). Attack identification for cyber-physical security in dynamic games under cognitive hierarchy. *IFAC-PapersOnLine*, *56*(2), 11223-11228.
46. McCarthy, J. (1959). Programs with common sense
47. McCarthy, J. (1978). History of LISP. In History of programming languages (pp. 173-185
48. McAlaney, J., Hills, P. J., & Cole, T. (2024). Forensic Perspectives on Cybercrime: Human Behaviour and Cybersecurity. Taylor & Francis., J., Hills, P. J., & Cole, T. (2024). Forensic Perspectives on Cybercrime: Human Behaviour and Cybersecurity. Taylor & Francis
49. Mester, L. J. (2019). Cybersecurity and financial stability. Speech at the Federal Reserve Bank of Cleveland, Cleveland, Ohio, 21
50. Mishra, Shailendra. 2023. "Exploring the Impact of AI-Based Cyber Security Financial Sector Management" Applied Sciences 13, no. 10: 5875. https://doi.org/10.3390/app13105875
51. Mohamadou, Y., Halidou, A., & Kapen, P. T. (2020). A review of mathematical modeling, artificial intelligence and datasets used in the study, prediction and management of COVID-19. *Applied Intelligence*, *50*(11), 3913-3925.
52. Mohammed, Y. B., Badara, M. S., & Dan'azumi, H. (2024). An Intelligence-Based Cybersecurity Approach: A Review. Journal of Intelligent Communication, 4(1), 32-43
53. Nabiebu, M., Otu, M. T., & Eja, A. E. (2024). Enhancing Efforts to Combat Fraud: Addressing Challenges and Proposing Reforms. Alkebulan: A Journal of West and East African Studies, 4(1), 18-29.
54. Nwankwo, W., Chinedu, P. U., Masajuwa, F. U., Njoku, C. C., & Imoisi, S. E. (2023). Adoption of i-voting infrastructure: addressing network-level cybersecurity breaches. *Electronic Government, an International Journal*, *19*(3), 273-303.
55. Odumesi, J. O. (2014). Combating the menace of cybercrime. International Journal of Computer Science and Mobile Computing, 3(6), 980-991.
56. Owolabi, S. (2010, September 29). Fraud and Fraudulent Practices in Nigeria Banking Industry. African Journals Online, 4(3). https://doi.org/10.4314/afrrev.v4i3.60263
57. Papadopoulos, N. (2021). How Secure are you Online?: A Cybersecurity Assessment of the Recommendations Provided to Swedish Citizens.
58. Payne, B. K. (2020). Defining cybercrime. The Palgrave Handbook of International Cybercrime and Cyber Deviance, 3-25.

59. Reis, O., Oliha, J.S., Osasona, F., & Obi, O.C. (2024). Cybersecurity dynamics in Nigerian banking: trends and strategies review. Computer Science & IT Research Journal, 5(2), 336-364. https://dx.doi.org/10.51594/csitrj.v5i2.761
60. Ruatta, B. T., Piekarsa, G. J., Christian, J., Edbert, I. S., & Gunawan, A. A. S. (2023, August). Cyber Security in Smart Cities and Its Challenges: A Systematic Literature Review. In *2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS)* (pp. 87-91). IEEE.
61. Roessner, D. (2000). Quantitative and qualitative methods and measures in the evaluation of research. Research Evaluation, 9(2), 125-132
62. Sabillon, R. (2022). National Cybersecurity Strategies. In Research Anthology on Business Aspects of Cybersecurity (pp.500-513). IGI Global. https://dx.doi.org/10.4018/978-1-6684-3698-1.ch023
63. Sasmal, S. (2021). Preventing Card Fraud and Scam Using Artificial Intelligence.
64. Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, 11-20.
65. Schatz, Daniel; Bashroush, Rabih; and Wall, Julie (2017) "Towards a More Representative Definition of Cyber Security," Journal of Digital Forensics, Security and Law: Vol. 12: No. 2, Article 8. DOI: https://doi.org/10.15394/jdfsl.2017.1476
66. Setiawan, Roy and Cavaliere, Luigi Pio Leanardo and Koti, Kartikey and Ogunmola, Gabriel Ayodeji and Jalil, Nasir Abdul and Chakravarthi, M. Kalyan and Rajest, S. Suman and Regin, R. and Singh, Sonia (2021) The Artificial Intelligence and Inventory Effect on Banking Industrial Performance. https://www.tojqi.net/index.php/journal/article/view/3258
67. Sidik, M. (2020). Cyber security applied for financial sector in Indonesia. Journal Pajak dan Bisnis (Journal of Tax and Business), 1
68. Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system: A review of the literature. Online Information Review, 41(2), 171-184.
69. Schjolberg, S. (2020). *The history of cybercrime* (Vol. 13). BoD–Books on Demand.
70. Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-centric Computing and Information Sciences*, *8*(1), 1-22.
71. Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., & Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems*, *246*, 108709.
72. Taplin, R. (Ed.). (2016). Managing cyber risk in the financial sector: Lessons from Asia, Europe and the USA. Routledge
73. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. *IEEE journal of selected topics in signal processing*, *14*(5), 910-932.
74. Vieira, A., & Sehgal, A. (2017). How banks can better serve their customers through artificial techniques. In *Digital marketplaces unleashed* (pp. 311-326). Berlin, Heidelberg: Springer Berlin Heidelberg.
75. Urbas, G. (2019). Legal perspectives on cybercrime. In Research Handbook on Transnational Crime (pp. 316-326). Edward Elgar Publishing
76. Wang, Z., Dong, Y., Xiang, Z., & Cheng, S. (2024). An Overview of Artificial Intelligence Security Issues. Artificial Intelligence Technologies and Applications, 131-139.
77. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report
78. https://commission.europa.eu/publications/proposal-cybersecurity-regulation_en
79. https://www.unodc.org/unodc/en/cybercrime/home.html
80. https://thehackernews.com
81. https://www.sophos.com
82. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
83. https://au.int/en/pressreleases/20240522/african-union-strengthens-investigation-capabilities-virtual-assets-and

Appendix. 1

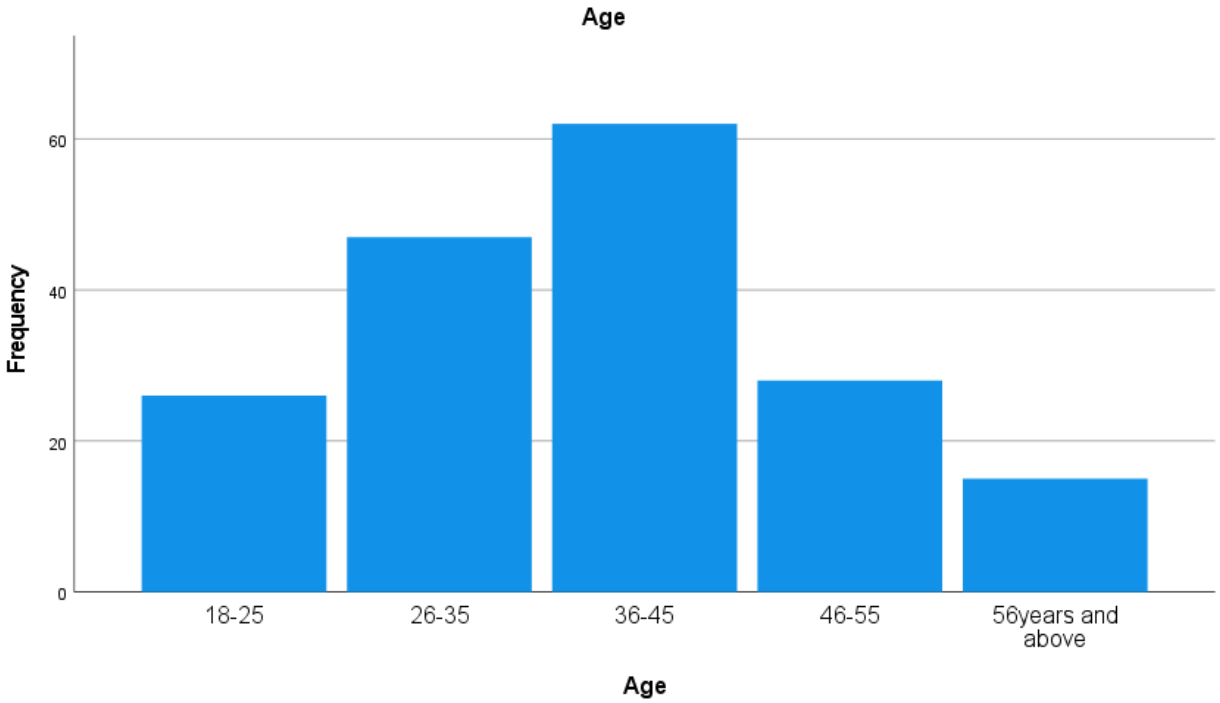
Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	117	65.7	65.7	65.7
	Female	61	34.3	34.3	100.0
	Total	178	100.0	100.0	



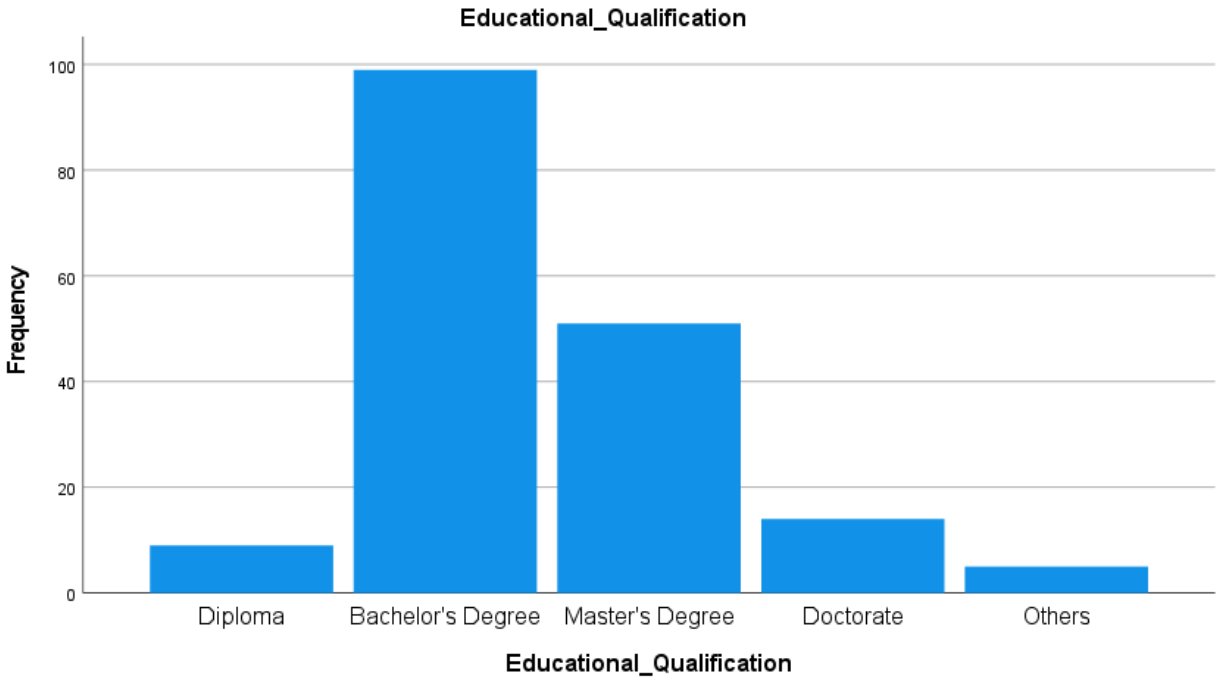
Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	26	14.6	14.6	14.6
	26-35	47	26.4	26.4	41.0
	36-45	62	34.8	34.8	75.8
	46-55	28	15.7	15.7	91.6
	56years and above	15	8.4	8.4	100.0
	Total	178	100.0	100.0	



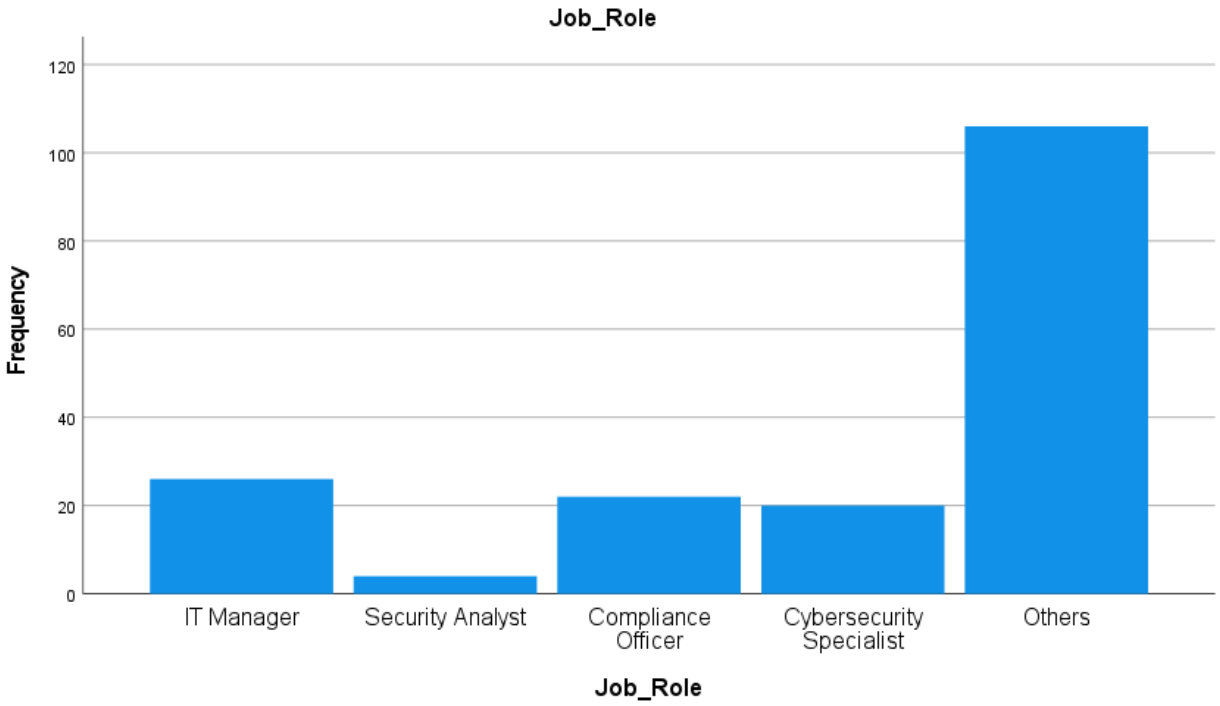
Educational_Qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	9	5.1	5.1	5.1
	Bachelor's Degree	99	55.6	55.6	60.7
	Master's Degree	51	28.7	28.7	89.3
	Doctorate	14	7.9	7.9	97.2
	Others	5	2.8	2.8	100.0
	Total	178	100.0	100.0	



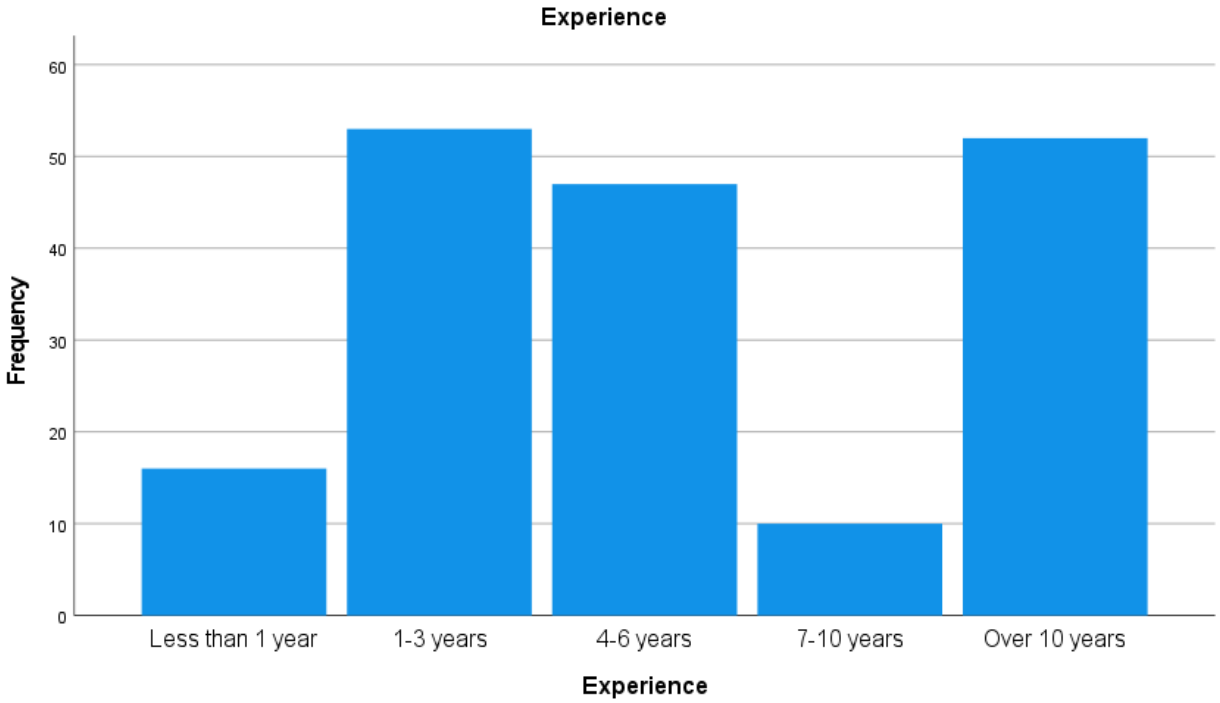
Job_Role

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT Manager	26	14.6	14.6	14.6
	Security Analyst	4	2.2	2.2	16.9
	Compliance Officer	22	12.4	12.4	29.2
	Cybersecurity Specialist	20	11.2	11.2	40.4
	Others	106	59.6	59.6	100.0
	Total	178	100.0	100.0	



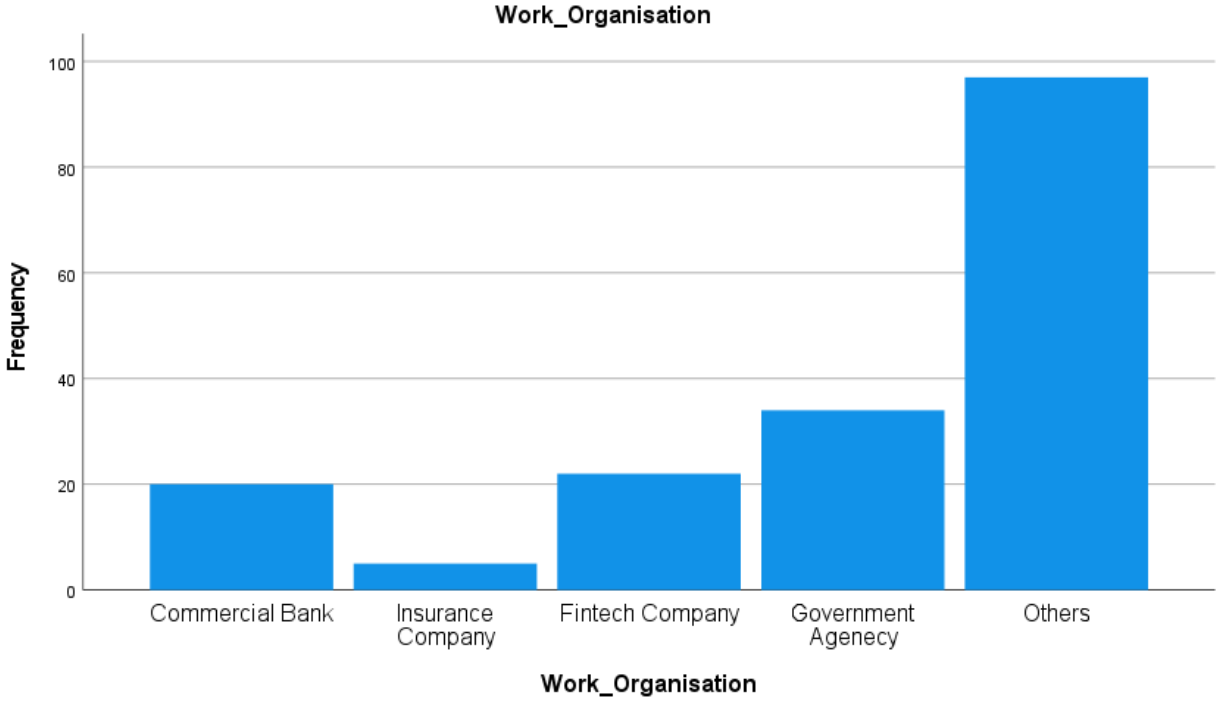
Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1 year	16	9.0	9.0	9.0
	1-3 years	53	29.8	29.8	38.8
	4-6 years	47	26.4	26.4	65.2
	7-10 years	10	5.6	5.6	70.8
	Over 10 years	52	29.2	29.2	100.0
	Total	178	100.0	100.0	



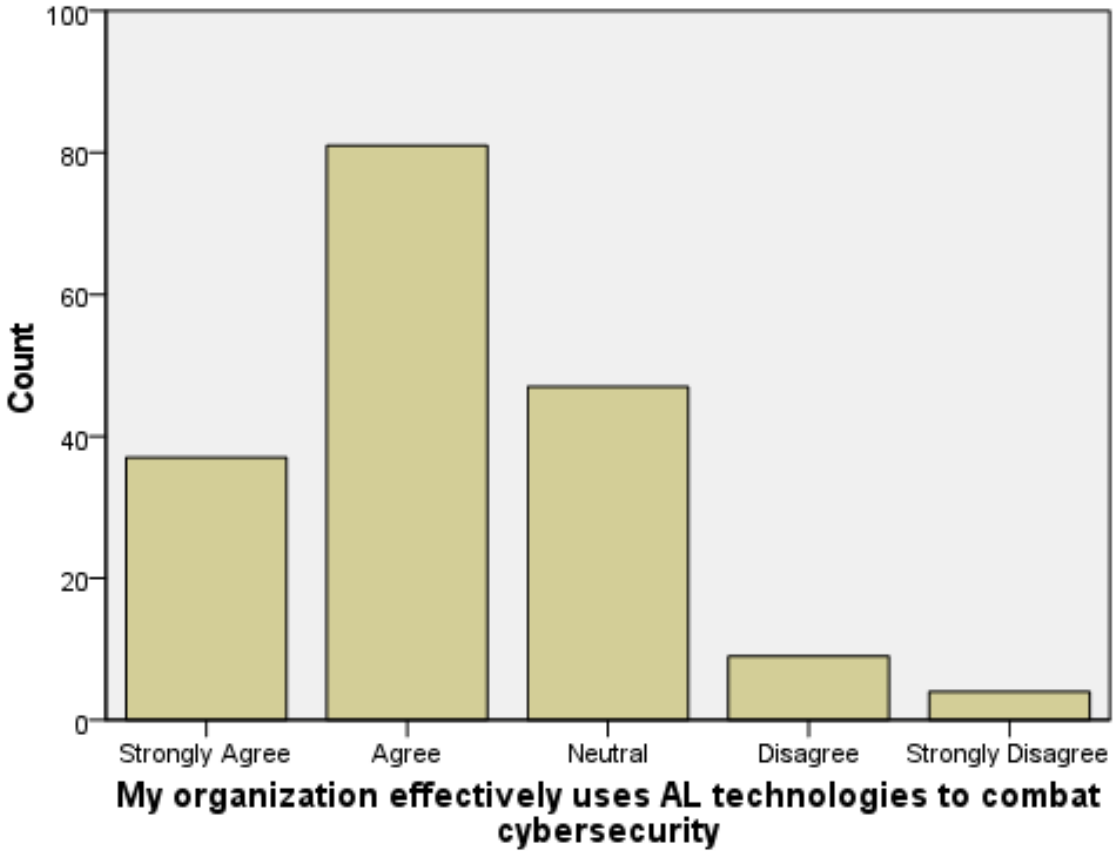
Work_Organisation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Commercial Bank	20	11.2	11.2	11.2
	Insurance Company	5	2.8	2.8	14.0
	Fintech Company	22	12.4	12.4	26.4
	Government Agencies	34	19.1	19.1	45.5
	Others	97	54.5	54.5	100.0
	Total	178	100.0	100.0	



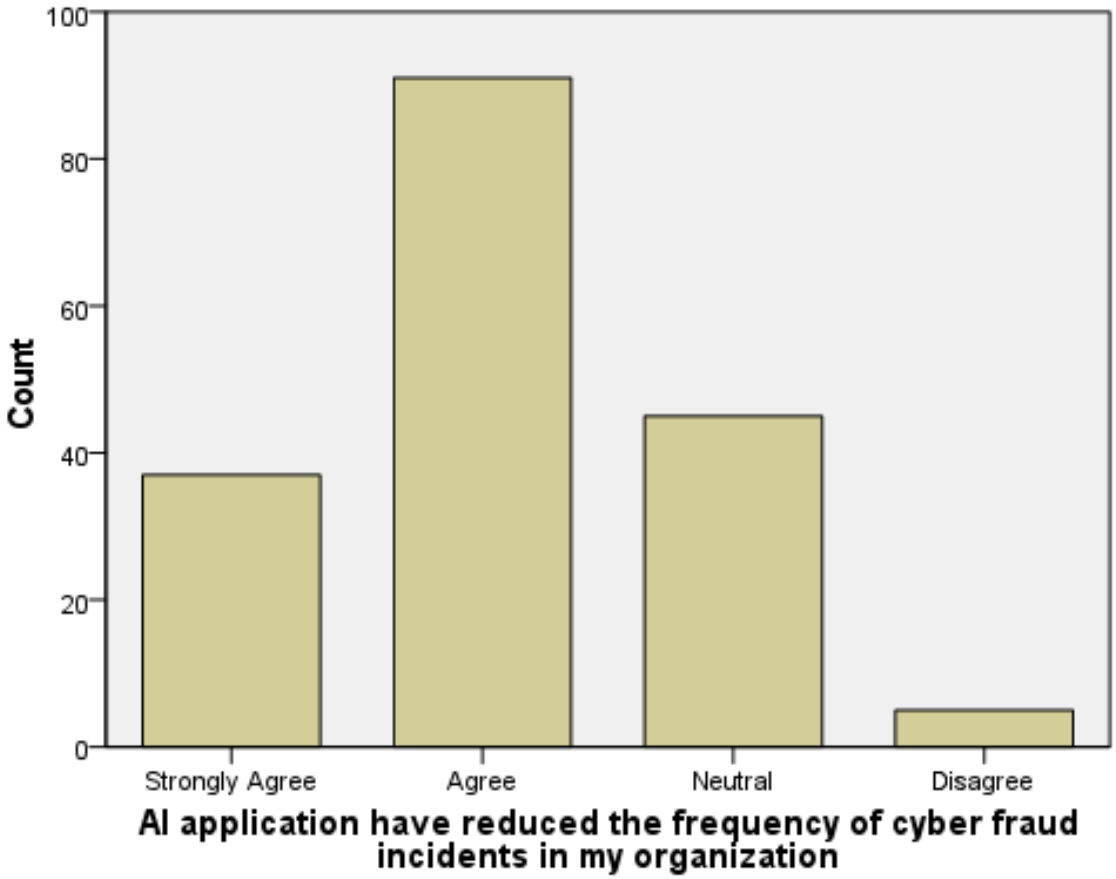
My organization effectively uses AL technologies to combat cybersecurity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	37	20.8	20.8	20.8
	Agree	81	45.5	45.5	66.3
	Neutral	47	26.4	26.4	92.7
	Disagree	9	5.1	5.1	97.8
	Strongly Disagree	4	2.2	2.2	100.0
	Total	178	100.0	100.0	



AI application have reduced the frequency of cyber fraud incidents in my organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	37	20.8	20.8	20.8
	Agree	91	51.1	51.1	71.9
	Neutral	45	25.3	25.3	97.2
	Disagree	5	2.8	2.8	100.0
	Total	178	100.0	100.0	



emails: A study on the persuasiveness of AI-generated phishing emails versus human methods phishing emails: A study on the persuasiveness of AI-generated phishing emails versus human methods to create phishing emails: A study on the persuasiveness of AI-generated phishing emails versus human methods

Appendix. 2

RESEARCH QUESTIONNAIRE

A pre-approval request on the research questionnaire on the Use of Artificial Intelligence application in the prevention of Cyber fraud and critical asset incidents in Nigeria and the financial sector·

Please help to complete this research survey for academic purpose on the use of artificial intelligence application in the prevention of cybercrime incidents in Nigeria critical assets and the financial sector. Your answers would be treated with confidentiality. It is an open/closed ended questionnaire with options to choose and your opinion on the use of artificial intelligence in your organization.

Section 1: Demographic Information

1. **Gender:** Male Female

2. **Age:** 18-25 26-35 36-45 46-55 56 and above

3. **Educational Qualification:** Diploma Bachelor's Degree. Master's Degree

   Doctorate Other (Please specify): _____

4. **Job Role:** IT Manager Security Analyst Compliance Officer

   Cybersecurity Specialist Other (Please specify): _____

5. **Years of Experience in the Financial Sector:** Less than 1 year 1-3 years

   4-6 years 7-10 years Over 10 years

6. **Please indicate the type of organization you work for:** Commercial Bank insurance Company

   (FinTech) Company. Government Agency Other (Please specify): _____

Section 2: Types of AI Technologies Currently Utilized in Cybersecurity

1. **Which of the following AI technologies are been currently used in your organization for cyber-Crime management** Machine Learning Algorithms Natural Language Processing (NLP)

   Predictive Analytics Automated Threat Detection Systems. Behavioural Analysis Tools

   Other (Please specify): _____

2. **Please rate your decision with the following statement: "My organization effectively uses AI technologies to combat cybercrime incidents …….** Strongly Agree Agree

   Neutral Disagree Strongly Disagree

3. **The implementation of the use of AI applications has the performance to detect cybercrime incidents in critical infrastructure ----------**

Strongly Agree Agree Neutral

Disagree Strongly Disagree

Section 3: Limitations of AI Implementation

4. The flagging rate of false positives in AI driven Artificial intelligence is a negative effect in the accuracy and detection of cybercrime incidents……..
Strongly agree Agree Neutral

Disagree Strongly Disagree

5. To what extent to do believe that artificial intelligence tools is cost effective compared to traditional method in detecting cybercrime incidents…….
Strongly Agree Agree Neutral

Disagree Strongly Disagree

6. To what extent do you agree with the following statement: "Implementing AI in cybersecurity presents significant challenges**."** Strongly Agree Agree

Neutral Disagree Strongly Disagree

Section 5: Impact of AI-Based Cybersecurity Measures

7. AI-based cybersecurity measures have improved the overall security posture in managing critical assets……..:
Strongly Agree Agree Neutral

Disagree Strongly Disagree

8. The implementation of AI in cybersecurity is quick to detection of cybercrime incidents in critical infrastructure ……..
Strongly Agree Agree Neutral

Disagree Strongly Disagree

9. AI-based model have effectively contributed in combating cybercrime incident….. Strongly Agree Agree

Neutral Disagree Strongly Disagree

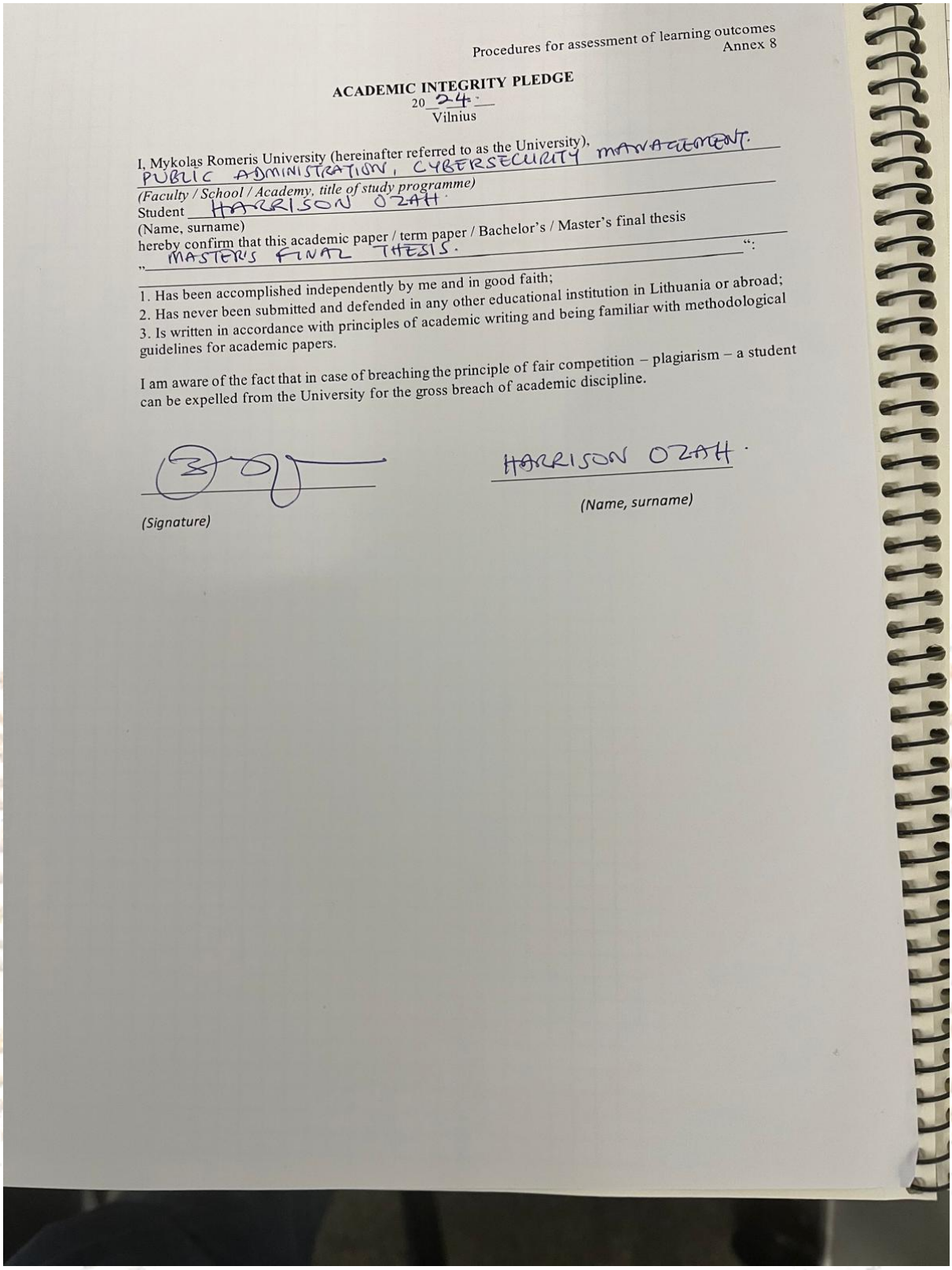
10. How would you rate the impact of AI in incident resolution in cybercrime incident…..
Strongly agree **Agree**

Neutral Disagree Strongly

Disagree

11. What additional AI capabilities would you like to see implemented in your organization's cybersecurity systems?.....
12. In your opinion, what are the most common cybercrime incidents you have suffered in organization?.....
13. Do you believe AI can fully replicate the human intervention in managing cyber fraud incidents? ……S
14. What improvements would you recommend for AI-powered cybersecurity solutions in your organization?.....
15. What are your thoughts on the role of AI in shaping the future of cybersecurity**? ……..**

INTERNATIONAL JOURNAL FOR ENGINEERING RESEARCH TECHNIX
TIJER
OPEN ACCESS JOURNAL



Procedures for assessment of learning outcomes
Annex 8

ACADEMIC INTEGRITY PLEDGE

20 24

Vilnius

I, Mykolas Romeris University (hereinafter referred to as the University),
PUBLIC ADMINISTRATION, CYBERSECURITY MANAGEMENT.
(Faculty / School / Academy, title of study programme)
Student HARRISON OZAH.
(Name, surname)
hereby confirm that this academic paper / term paper / Bachelor's / Master's final thesis
"MASTERS FINAL THESIS. ":

1. Has been accomplished independently by me and in good faith;
2. Has never been submitted and defended in any other educational institution in Lithuania or abroad;
3. Is written in accordance with principles of academic writing and being familiar with methodological guidelines for academic papers.

I am aware of the fact that in case of breaching the principle of fair competition – plagiarism – a student can be expelled from the University for the gross breach of academic discipline.

(Signature)

HARRISON OZAH.

(Name, surname)