WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Intelligent Cybershield: Developing Artificial Intelligence for Secure Internet Banking

[1]Idam, Eugene Oko, [2]Iroh, Chioma U.; [3]Onuohah, Frank Lotanna; [4]Onyeonwu, Chekwube Chukwunwendu

[1]Department of Electrical/Electronics Engineering, Joseph Sarwuan Tarka University, Makurdi, Benue state, Nigeria.
[2] Department of Electrical/Electronics Engineering, Abia state university, Uturu, Abia State, Nigeria,
[3] Osten Laboratory Limited, PortHarcourt, Rivers State, Nigeria
[4]Unegbe Ventures Investment Limited, Ogbunike, Anambra state, Nigeria.
Email: idmeugene285@gmail.com;

ABSTRACT:

The rapid growth of internet banking has increased the vulnerability of financial transactions to cyber-attacks, resulting in significant economic losses. To counter this threat, this research focuses on developing an Artificial Intelligence (AI) system specializing in cybercrime security for internet banking. The proposed AI framework integrates machine learning algorithms, natural language processing, and anomaly detection to identify and prevent fraudulent transactions in real-time. The system analyzes user behavior, transaction.

The increasing adoption of internet banking has raised concerns about security and privacy in Nigerian banking system. Cybercriminals are using sophisticated techniques to compromise online banking systems, resulting in financial losses and damage to customer trust. To address this challenge, we propose the development of an "Intelligent Shield" - an artificial intelligence (AI) system designed to detect and prevent cyber threats in internet banking.

The Intelligent Shield system utilizes machine learning algorithms to analyze user behavior, transaction patterns, and system vulnerabilities to identify potential security threats. The system can detect anomalies in real-time, alerting bank security teams to take prompt action. Additionally, the Intelligent Shield system can predict and prevent fraudulent activities, such as phishing attacks and account takeovers.

The development of the Intelligent Shield system involves several stages, including data collection, algorithm training, and system integration. We evaluate the performance of the system using a dataset of real-world banking transactions and demonstrate its effectiveness in detecting and preventing cyber threats.

The Intelligent Shield system has the potential to revolutionize internet banking security, providing a robust and proactive defense against cybercriminals. Its implementation can enhance customer trust, reduce financial losses, and improve the overall security posture of online banking systems. This survey six banks in Nigeria and generated a data that proposes the adoption of artificial intelligent in the protection of the banking industries

Keywords: intelligent shield, Artificial Intelligence, Internet Banking, Cybersecurity, Fraud Detection, Anomaly Detection.

1. Introduction:

What Is Artificial Intelligence (AI)?: Artificial intelligence (AI) technology allows computers and machines to simulate human intelligence and problem-solving tasks (THE INVESTOPEDIA TEAM Updated April 09, 2024) The ideal characteristic of artificial intelligence is its ability to rationalize and take action to achieve a specific goal. AI research began in the 1950s and was used in the 1960s by the United States Department of Defense when it trained computers to mimic human reasoning. A subset of artificial intelligence is machine learning (ML), a concept that computer programs can automatically learn from and adapt to new data without human assistance.

Algorithms are part of the structure of artificial intelligence, where simple algorithms are used in simple applications, while more complex ones help frame strong artificial intelligence. Artificial intelligence technology is apparent in computers that play chess, self-driving cars, and banking systems to detect fraudulent activity.

How Artificial Intelligence (AI) Works: Artificial intelligence commonly brought to mind the implementation of robots. As technology evolved, previous benchmarks that define artificial intelligence became outdated. Technologies that enable Artificial Intelligence include:

-SSAS. "Artificial Intelligence."

-Computer vision enables computers to identify objects and people in pictures and photos.

- Natural language processing (NLP) allows computers to understand human language

-Graphical processing units are computer chips that help computers form graphics and images through mathematical calculations.

-The Internet of Things is the network of physical devices, vehicles, and other objects embedded with sensors, software, and network connectivity, that collect and share data.

-Application programming allows two or more computer programs or components to communicate with each other.

-Algorithms often play a part in the structure of artificial intelligence, where simple algorithms are used in simple applications, while more complex ones help frame strong artificial intelligence.

Types of Artificial Intelligence

Narrow AI: Also known as Weak AI, this system is designed to carry out one particular job. Weak AI systems include video games like personal assistants like Amazon's Alexa and Apple's Siri. Users ask the assistant a question, and it answers it for you.

General AI: This type includes strong artificial intelligence systems that carry on the tasks considered to be human-like. They tend to be more complex and complicated and can be found in applications like self-driving cars or hospital operating rooms.

Super AI is a strictly theoretical type of AI and has not yet been realized. Super AI would think, reason, learn, and possess cognitive abilities that surpass those of human beings.

Using Artificial Intelligence

Artificial intelligence can be applied to many sectors and industries, including the healthcare industry for suggesting drug dosages, identifying treatments, and aiding in surgical procedures in the operating room.

Other examples of machines with artificial intelligence include computers that play chess and self-driving cars. AI has applications in the financial industry, where it detects and flags fraudulent banking activity. Applications for AI can help streamline and make trading easier.

In 2022, AI entered the mainstream with applications of Generative Pre-Training Transformer. The most popular applications are OpenAI's DALL-E text-to-image tool and ChatGPT. According to a 2024 survey by Deloitte, 79% of respondents who are leaders in the AI industry, expect generative AI to transform their organizations by 2027.

What Is Reactive AI? Reactive AI is a type of Narrow AI that uses algorithms to optimize outputs based on a set of inputs. Chess-playing AIs, for example, are reactive systems that optimize the best strategy to win the game. Reactive AI tends to be fairly static, unable to learn or adapt to novel situations.

What Are the Concerns Surrounding the Use of AI? Many are concerned with how artificial intelligence may affect human employment. With many industries looking to automate certain jobs with intelligent machinery, there is a concern that employees would be pushed out of the workforce. Self-driving cars may remove the need for taxis and car-share programs, while manufacturers may easily replace human labor with machines, making people's skills obsolete

The Bottom Line: Artificial Intelligence (AI) is an evolving technology that tries to simulate human intelligence using machines. AI encompasses various subfields, including machine learning (ML) and deep learning, which allow systems to learn and adapt in novel ways from training data. It has vast applications across multiple industries, such as healthcare, finance, and transportation. While AI offers significant advancements, it also raises ethical, privacy, and employment concerns

The escalating number of online banking frauds, identity thefts, and data breaches has raised concerns about the security and integrity of internet banking systems. Traditional security measures, such as firewalls and encryption, are no longer sustainable. The advent of internet banking has revolutionized the way we manage our finances, offering unparalleled convenience and accessibility (Kumar et al., 2022). However, this shift has also introduced new vulnerabilities, making it a prime target for cybercriminals (Ahmed et al., 2021). As the threat landscape continues to evolve, traditional security measures are no longer sufficient to protect against the sophisticated attacks that put sensitive information and financial assets at risk (Chakraborty et al., 2022).

In this context, Artificial Intelligence (AI) emerges as a promising solution to bolster cybercrime security in internet banking. AI's capabilities in machine learning, pattern recognition, and real-time analysis make it an ideal technology to detect and prevent fraudulent activities. By developing AI systems that specialize in cybercrime security, internet banking can become more resilient, secure, and trustworthy.

This research focuses on the development and review of relevant articles and journals of an AI system that can effectively identify, prevent, and respond to cyber threats in internet banking. By exploring the latest advancements in AI and cybersecurity. This study aims to create a robust and adaptive security framework that can safeguard the integrity of online financial transactions and protect users from the ever-evolving landscape of cyber threats.

In response, the development of Intelligent Shield, an artificial intelligence (AI) powered cybersecurity system, is poised to transform the security landscape of internet banking (Jain et al., 2022). By harnessing the power of machine learning and advanced algorithms, Intelligent Shield detects and

prevents even the most subtle and complex threats in real-time, ensuring the integrity of online transactions and protecting users from financial fraud (Kumar et al., 2022)

Tayal et al (2022), explained more on the impact of AI on cybersecurity industry and how best to curb its vulnerabilities. It further buttressed the advantages of cyber security when AI is used and its effect on Bangladesh states.

This study carried out AI development research on hoe it could secure the banking sectors with a constructed questionnaires to drive home the result. It tends to tackle the knowledge of AI, obstacles arising in the use of AI, the language barrier, and the adoption of AI for advance internet banking security. The summary result are;

i) Nigerian private banks are yet to embrace AI POWERED system for the security and enhancement of internet banking.

ii) there is lack of modern technology and software engineering tools to anchor AI powered system.

iii) Government-owned banking hjjjon the queue of adoption of AI POWERED SYSTEM to secure the internet banking.

iv) Nigerian commercial banks have data leaks, insecure shield compared to government owned banks which accounts for the lack of AI POWERED SYSTEM.

v) The banks rejected the adoption of AI in their banking system due to lack of technology to handle the algorithm involved.

2. Literature Review and Hypothesis development

2.1 Application of AI in Nigerian banking sector.

The banking sector has witnessed so much significant transformation with the integration of Artificial Intelligence (AI) technologies. Among various applications, one of the most critical areas of focus is the development of intelligent shields for Internet banking. This literature review aims to explore the current landscape, challenges,

and future prospects of AI implementation in Internet banking security in Nigeria banks.

In Nigeria, businesses are keenly tapping into the potential of cutting-edge technologies to drive their growth strategies. According to Equinix's 2023 Global Tech Trends Survey, 47% of Nigerian businesses actively embrace interconnection, and over 90% are banking on artificial intelligence (AI) benefits to expand their operations, enhance efficiency, and stay competitive in the digital era. Moreover, Artificial Intelligence (AI) has significantly curbed banking fraud, particularly in the face of rising credit card fraud due to the expansion of e-commerce and online transactions. AI-driven fraud detection systems meticulously analyze customer behaviour, location, and spending patterns. These systems promptly activate security protocols upon detecting anomalies.

One of the primary applications of AI in Internet banking is fraud detection. AI algorithms, such as machine learning and deep learning, are employed to analyze vast amounts of transactional data in real-time, enabling the detection of fraudulent activities with high accuracy (Raza et al., 2020). These systems continuously learn from new data, improving their detection capabilities over time.

AI-driven authentication mechanisms play a crucial role in securing Internet banking transactions. Biometric authentication methods, including facial recognition and voice recognition, provide a more secure and user-friendly alternative to traditional password-based authentication (Swathi et al., 2019). AI algorithms analyze biometric data to ensure the identity of the user, mitigating the risk of unauthorized access.

Behavioral biometrics leverage AI algorithms to analyze user behavior patterns, such as typing speed, mouse movements, and navigation patterns, to authenticate users and detect potential security threats (Jain et al., 2020). By continuously monitoring user behavior, banks can detect anomalies indicative of fraudulent activities and intervene promptly. consequently, Ai driven chatbots plays a very good role in internet banking sector. AI-driven chatbots have become integral to Internet banking platforms, providing customers with instant assistance and support. These chatbots utilize natural language processing (NLP) and machine learning algorithms to understand customer queries and provide personalized responses (Huang et al., 2018). Additionally, AI-powered chatbots can assist customers in securely navigating through various banking services and processes. However, RPA technologies, powered by AI, streamline repetitive tasks in compliance and security processes, such as identity verification and regulatory reporting (Chuang et al., 2020). By automating these tasks, banks can enhance efficiency, reduce human error, and ensure compliance with regulatory requirements.

Despite the numerous benefits of AI in Internet banking security, several challenges persist. These include concerns regarding data privacy, algorithm bias, and cybersecurity threats targeting AI systems. Addressing these challenges requires a collaborative effort from banks, regulatory bodies, and AI developers to establish robust governance frameworks, systems and security measures.

In conclusion, the development of intelligent shields for Internet banking through AI represents a significant advancement in enhancing security, improving customer experience, and mitigating fraud risks. However, continuous innovation and collaboration are essential to overcome challenges and realize the full potential of AI in the banking sector. .

Hypothesis 1; Knowledge of artificial intelligence and its enhancement has a positive and significant effect on the adoption of internet banking security in Nigeria.

2.2 AI issues and implications/ cyberthreats.

The integration of Artificial Intelligence (AI) in the banking sector has brought about numerous benefits, including enhanced efficiency, improved customer experience, and better risk management. However, along with these advantages come various issues and implications, particularly concerning cybersecurity threats. This literature review explores the challenges and implications of AI implementation in the banking sector, focusing on cybersecurity concerns.

AI systems in banking heavily rely on vast amounts of data for training and decision-making processes. However, the collection and processing of sensitive customer information pose significant data privacy and security risks (Nami et al., 2020). Malicious actors may exploit vulnerabilities in AI algorithms or data breaches to gain unauthorized access to personal and financial data, leading to potential financial losses and reputational damage for banks.

Adversarial attacks pose a significant threat to AI systems deployed in banking applications. These attacks involve manipulating input data to deceive AI algorithms and produce incorrect outputs (Biggio et al., 2018). In the banking sector, adversarial attacks can be particularly damaging, as they may lead to erroneous decisions in credit scoring, fraud detection, or risk assessment processes, compromising the integrity and reliability of AI-driven systems.

AI algorithms used in banking applications may exhibit bias due to inherent biases in training data or algorithmic design. This bias can result in discriminatory outcomes, such as differential treatment of customers based on demographic factors (Dastin, 2021). Addressing algorithmic bias and ensuring fairness in AI systems is essential to maintain trust and transparency in banking operations.

The rapid advancement of AI technology in the banking sector has outpaced regulatory frameworks, leading to challenges in ensuring compliance with data protection and cybersecurity regulations (Fatima et al., 2021). Regulators face the task of updating existing regulations to address emerging AI-related risks effectively, while banks must navigate complex regulatory requirements to deploy AI solutions responsibly.

Cyber Threats and Vulnerabilities; AI-powered banking systems are vulnerable to a wide range of cyber threats, including malware attacks, phishing attempts, and ransomware campaigns (Kshetri, 2019). As cybercriminals increasingly leverage AI techniques to orchestrate sophisticated attacks, banks must continuously strengthen their cybersecurity measures, such as implementing robust authentication mechanisms, encryption protocols, and intrusion detection system. Alzoubi et al.(2022), this paper focuses on Cyber Security Threats on Digital Banking and its implication to the banking sector. I showcased the healthiness of cybersecurity in banking.

Khan et al,(2023); Utilizes Bio Metric System for Enhancing Cyber Security in Banking Sector: showing a systematic analysis on to curb cyber insecurities in banking sectors. ALMahadin et al, (2023), used Enabled Smart Banking AI and IoT and explained the challenges and opportunities in its usage.

Hypothesis 2*; Obstacles arising from using AI to secure the internet affects the banking sector positively and negatively in Nigerian.*

2.3 AI cyber protection in banking

AI-driven threat detection systems have become indispensable in safeguarding banking infrastructure against cyber threats. These systems utilize machine learning algorithms to analyze vast amounts of data in real-time, enabling the early detection and mitigation of security breaches and malicious activities (Vatanparvar et al., 2020). By continuously learning from new data patterns, AI algorithms enhance their ability to identify and respond to emerging cyber threats effectively.

Behavioral Biometrics for User Authentication; Behavioral biometrics, powered by AI, provide an additional layer of security in user authentication processes. These systems analyze unique behavioral patterns, such as typing speed, mouse movements, and navigation behavior, to verify the identity of users accessing banking services (Vasilomanolakis et al., 2019). By leveraging AI algorithms, banks can detect anomalies indicative of unauthorized access attempts and prevent fraudulent activities.AI-Driven Fraud Detection and Prevention; AI algorithms are instrumental in detecting and preventing various forms of fraud, including payment fraud, identity theft, and account takeover attacks. Through the analysis of transactional data, user behavior, and historical patterns, AI-powered fraud detection systems can identify suspicious activities and flag them for further investigation (Liu et al., 2021). Moreover, AI enables banks to deploy adaptive fraud prevention measures that evolve in response to emerging threats, thereby staying ahead of cybercriminals.

Adaptive Security Measures with AI; AI enables the implementation of adaptive security measures that dynamically adjust to evolving cyber threats and attack techniques. By analyzing vast datasets and threat intelligence feeds, AI systems can identify new attack vectors and vulnerabilities, allowing banks to proactively strengthen their defenses (Sharma et al., 2020). Additionally, AI-driven security orchestration and automation platforms streamline incident response processes, enabling faster threat containment and mitigation.

Challenges and Ethical Considerations; Despite the numerous benefits of AI cyber protection in banking, several challenges and ethical considerations persist. These include concerns regarding algorithmic bias, data privacy, and regulatory compliance (Vatanparvar et al., 2020). Addressing these challenges requires a holistic approach that combines technical expertise with ethical guidelines and regulatory frameworks to ensure the responsible development and deployment of AI-driven cybersecurity.

Rania Elouidan,(2023),In this essay, the hypothetico-deductive method is utilized to discover the several factors that influence the intents of Moroccan bankers to use AI technology. The PLS approach was used to evaluate the questionnaire data. Through the variables Perceived Ease of Employ and Perceived Utility, the factors Complexity of the Infrastructure, Compatibility, Conditions of Facilitation, and Managerial Support greatly impact the desire of Moroccan bank personnel to use AI technology.

Hypothesis 3; Employed AI and algorithms have vulnerabilities and positive effects in internet banking security in Nigeria

2.4 Developing AI to bridge the language barrier in securing the banking sector

Furthermore, using AI chatbots extends to offering personalised financial product recommendations to customers through AI-driven data analysis. These triggers targeted marketing of the bank's products and bolster sales improvement, according to PIOTECH. In the UAE, a pioneering virtual assistant named "EVA" has emerged as the inaugural digital aide in the Middle East and North Africa region. EVA possesses the remarkable ability to comprehend both Arabic and English languages, engaging users in natural conversations. Similarly, Kuwait has introduced "Banky," an AI-based virtual assistant that ensures secure, dependable, and swift interactions while addressing customer inquiries about banking services and products. In Egypt, the advent of "Zaki" has been announced, an intelligent virtual assistant heralded to enable clients to stay informed about the latest decisions from the Central Bank of Egypt and effortlessly explore diverse offerings across various banks.

***Hypothesis 4: AI bridging the gap in language interpretation of AI** skills **in Nigerian banking sector**.*

Figure 1 depicts the study's framework. In this study, five hypotheses were developed. The relationships between knowledge, obstacles, Ai algorithm, language barrier and adopting AI indicate hypotheses 1, 2, and 3. Furthermore, hypotheses 4 and 5, show that language barrier mediates the relationship between knowledge, obstacles arising, and the adoption of AI.

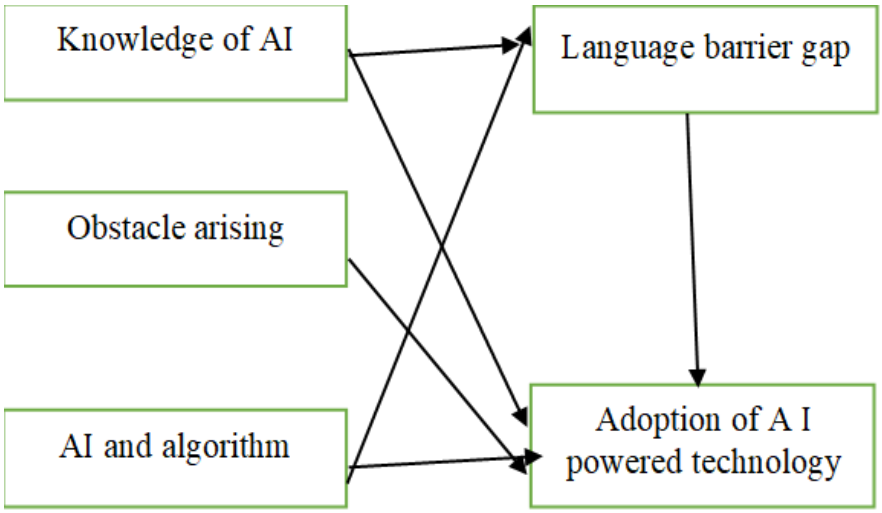


Figure 1: Frame work of the study

3.0 METHODOLOGY OF THE STUDY

3.1 Sample and Data collection through Survey

The sample data collection was done through survey of six selected banks in the central city of Makurdi Benue state of Nigeria. The banks are made up of government owned banks (NIRSAL

microfinance bank, first bank of Nigeria) and private banks (zenith bank, united bank of Africa, first city management bank, access bank) . The survey was done targeting the professionals with certain levels of education (graduates and post graduates) and their demographic profile determined before the survey as shown in Table I.

A questionnaire was constructed in three parts to ascertain the responses and as well to evaluate cyber insecurities within these selected banks (First bank of Nigeria (FBN), Zenith bank of Nigeria (ZBN), united bank of Africa (UBA), Access bank of Nigeria (ABN), NirsaL micro finance bank of Nigeria (NIRSAL), First city monument bank plc (FCMB). The constructed questions were analyzed using manual methods based on the available data generated

and the targeted audience were the professional ICT bankers (PIB) and software engineering developers and marketers working in the bank. This is because the structured questions are profession driven and to avoid wrong interpretations. They were stated thus and the result shown in table II,

3.2 Measurement

The data were gathered using a questionnaire developed using scales that had already been validated and adopted in the relevant literature. A total of three variables were used in the final survey that accommodated 10 questions. Our 10-item questionnaire satisfies the minimum criteria for measurement on three scale questions.

3.3 Data Analysis Technique

Due to having a "small sample size", "normal data", and "complex models", the Matlab tools of version 2021 version was used to generate the charts and tables for analysis.

3.4 Part 1:

How do AI-enhanced cyber security affects your bank on the below headings?

i. Address vulnerability

ii. helps solving major cyber security problem

iii. Cross channel deployment

3.5 Part 2:

How do Obstacles for using AI for improving security affects your bank?

i Need to train employes

ii lack of compatibility

iii Complexity

iv Inefficient and creates a potential security

3.6 Part 3:

How do Employed AI and algorithm have vulnerability in your banks?

i. Redundancy

ii. Data accumulation

iii. chats bot privacy and leaks

iv. coding error.

3.7 Findings and discussion;

Nigeria is presently one of the most populous and technologically disadvantaged countries in the world Nigeria (Nigerian journal of technology, pp.234). In light of their technology management strategies and dedication to sustainable innovation, the leading certified government and private banks in this research hope to learn how they adopt AI and its internet banking security development. It may be useful to comprehend the specific situation of technology practices and provide policy implications. The researchers asked permission from the top managers of the banks so that they may participate in our study as research subjects.

A representative sample of the bank responded to the survey. In this regard, the research model and results were validated using data from owners/top managers of the respective banks (the capital city of Benue state, Makurdi, Nigerian). An original data-gathering method was applied in this investigation.

The demographic breakdown the profile of the respondents is shown in Table I.

Characteristics	Frequency	Percentage	Age	Marital status	
Gender			20-50 years	Married	Single
Male	40	20	46	26	38

Female	30	15	49	44	29
Educational level					
Graduate	60	50	80	13	8
Postgraduate	50	35	35	23	20

Table 1: Respondent demographic profile

According to Table 1, 40percent , 30percentt of respondents were male and female, 20 per cent and 15 were between the ages of 20 and 50, 40, 26per cent and 38 percent were married and single among the male, while 44 and 29 percentage among female were married and single. 50 per cent had postgraduate degrees, 35 had degree, 80 per cent of postgraduate had 20–50 years age of foundation after establishment,20 -50 years of age had postgraduate at 35 years.

4.0 SCIENCIOMETRIC ANALYSIS OF THE RESULT:

MATLAB tools was used to analyze the data collected for effective distribution of information. A bar chart was developed for the various selected six banks. The characteristics of each bank were explained with regard to the constructed questionnaire. The data was calculated through manual calculation method And values distributed as show below.

Ai for enhancing cyber security	**Bank responses in percentage**					
	NIRSAL	ZBN	FCMB	UBA	ACCESS	FBN
i. address vulnerability	40%	30%	25%	45%	43%	46%
ii. help solving banking cyber security problem	45%	20%	30%	15%	25%	15%
iii. cross channel deployment	10%	12%	18%	19%	15%	22%
Obstacles for using AI for improving security						
i. need to train employees	5%	25%	28.6%	30%	25%	9%
ii. lack of compatibility	5%	30%	30%	25%	14%	15%
iii. complexity	25%	30%	35%	40%	25%	20%
iv. Insufficient and creates a potential security	10%	32%	22%	35%	23%	12%
Employed AI algorithms have vulnerabilities						
i. redundancy	12%	15%	12.8%	25%	10%	8%
ii. accumulation of data	45%	36%	34%	23%	24%	34%
iii. Chat bot privacy and leaks	43%	14%	33%	30%	28%	45%
iv. Fictious data	4%	35%	37%	30%	28%	10%
v. coding error	23%	16%	14%	31%	20%	23%

Result: Table 1I

4.1 Result of part one structured question:

The percentage output of the effect of AI in combating insecurity in the five selected banks in Nigeria is high and more especially the government-controlled banks (NIRSAL AND FBN) because of their proper application and good monitoring system. The commercial banks UBA, FCMB and ZBN revealed to be prone to attacks and internet insecurity, hence there is high level of vulnerability of the banks in Nigeria due to improper use of AI, not knowing how to secure the banking data activities.

4.2 Results of part two structured question:

the four commercial banks UBA, ACCESS, ZBN, FCMB scored high percentage value in their lack of man power training, compatibility in software engineering usage and development of complex software not properly tested before purchase leading to inefficiency creation in the system. 25% insecurity existence of UBA bank is catastrophic to the financial existence of the bank. This discovery if not guided will scare away investors and customers in Nigerian banking sectors.

4.3 Results of part three structured questions.

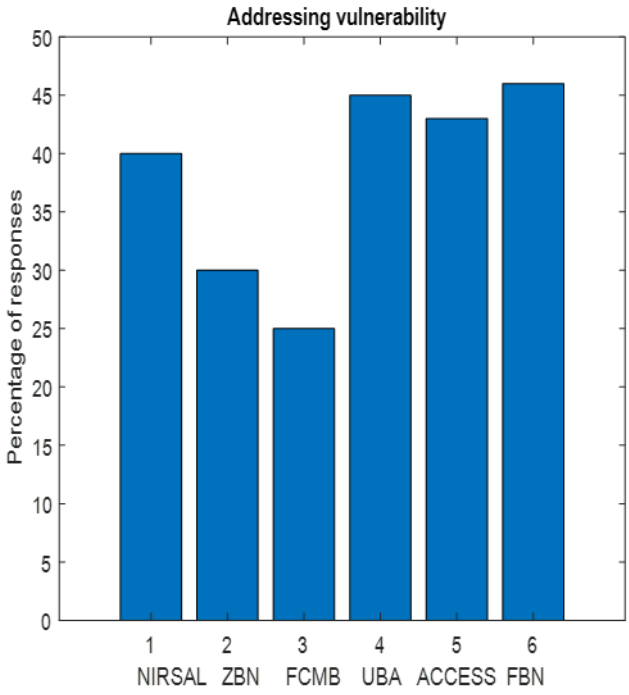
In this part, there is low percentage redundancy of Nigerian banks, the privacy of data and its leakage is high among the government owned banks NIRSAL and FBN) at 43% and 45% showing how vulnerable are its banking activities and poses a risk to investors.

There is a lot of challenges and threats affecting internet banking and software security. Its counterpart commercial banks have good controlled data leaks and information. Fictious information is much in the commercial banks recording 35%, 37%, 30% and 28% for ZBN, FCMB, UBA and ACCESS. This result is due to non-controlled activities in the private sector.

From the part one questions under addressing of vulnerability, the risk of banks in handling public fund and internet banking are high. It reviews fear on the part of customers regarding their fund. The FBN and UBA tops the list and needs to be handled.

The bar chart was further used to determine the percentage rate of vulnerabilities as illustrated in Figure 2. A bar chart of percentage respondents was plotted against the six selected banks to generate the vulnerabilities of the banks

Figure 2



From Figure 2, NIRSAL stands a better chance of resolving cybersecurity issues more than any of the banks followed by FBN UBA, FCMB and ACCESS bank.

Figure 3 introduces the problem-solving skills of insecurity and the rates at which internet banking securities with AI powered system. The variation rates the securities of the banks which could resolved by using AI powered system.

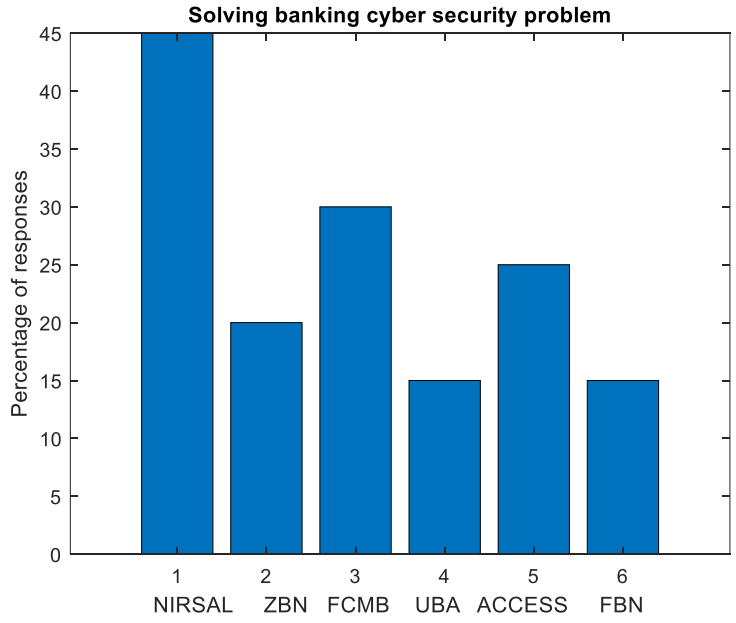


Figure 3

There is high need to train employees on the proper use of AI to secure the banking sector especially employes from ZBN,FCMB,UBA, and ACCESS banks.

Figure 4 explains the need to train employees to enable them handle the growing AI skills and operation.

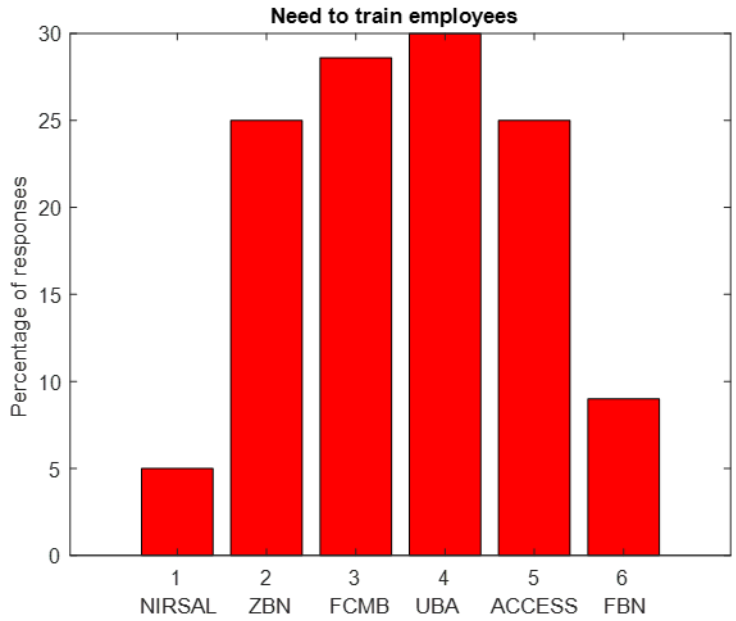


Figure 5 shows the compatibility of the AI powered systems and their adoption by the banks and how it affects it.

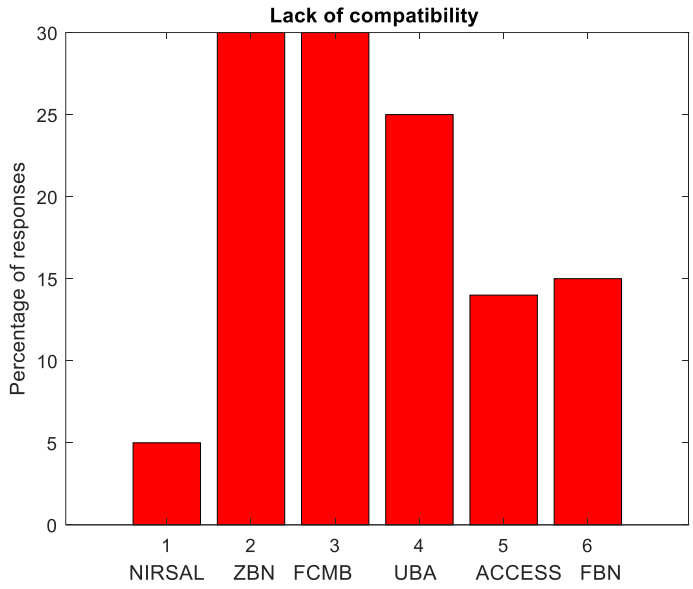


Figure 5

From Figure5, ZBN, FCMB and UBA lacks the modern AI tool to combat internet security to banking service, hence their tools are not compatible to the AI.

Figure 6 shows the redundancy of some banks on the application of AI powered system s in the banking sector. Its effects on banks are enormous.

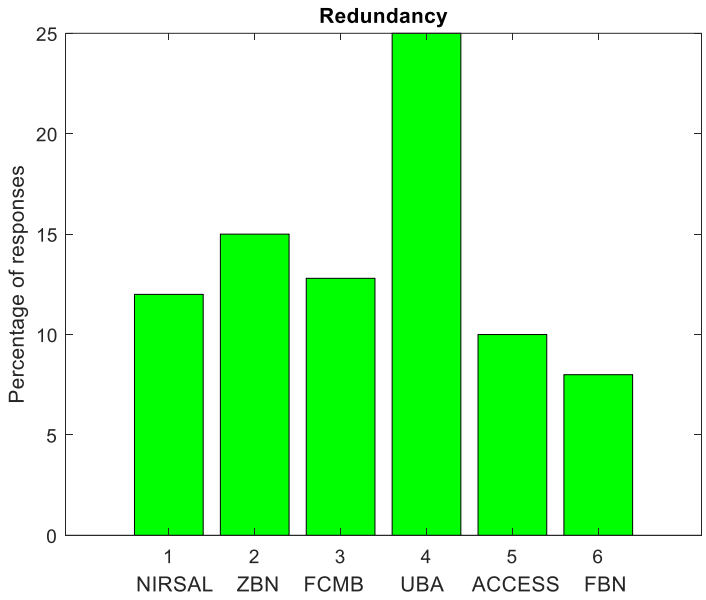


Figure 6

Figure 7 shows the data accumulation of in the use of AI powered system and how to handle them.

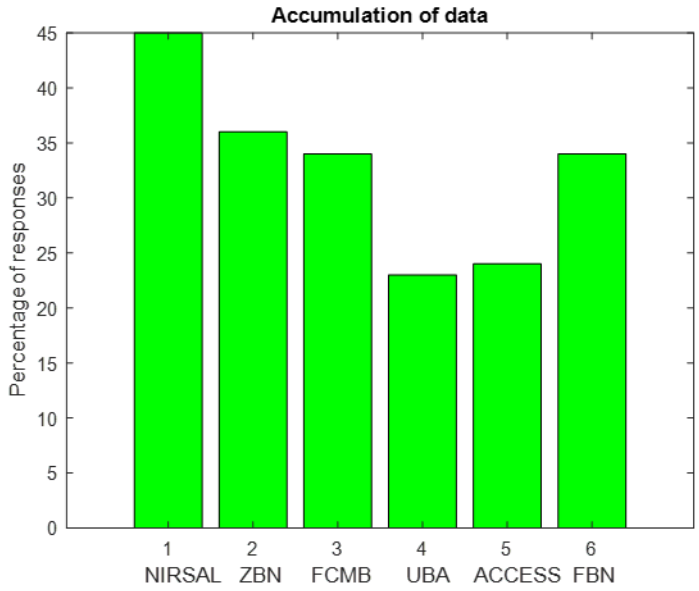


Figure 7

UBA is highly redundant in terms of their designed algorithm to secure internet banking. There is need for them to develop a special AI compliance system for combating banking internet insecurity. Some banks accumulate more data than any other banks. FBN and Nirsal bank ranked highest in data accumulation.

4.4 SUMMARY OF RESULTS:

The table 3 below gives an overview of the six respondents results concerning the use of AI to secure the banking sector and shield from hacker and cracker of the internet.

Hypothesis (H)	**Relationship**	**Decision**
H_1-Knowledge	Supported	Supported
H_2-obstacles arising	Indifferent or not interested	Supported
H_3- AI and algorithm	Reject technology	Rejected
H_4-language gap	Supported	Supported

Table 3:

The Table 3 summarized the relationship, acceptance and rejection of AI powered technology in Nigerian banking system. This enabled the researcher to determine how well AI technology could be implemented in the country bearing in mind the knowledge limitations, obstacles and language gaps.

i)Nigerian private banks are yet to embrace AI POWERED system for the security and enhancement of internet banking.

ii)there is lack of modern technology and software engineering tools to anchor AI powered system.

iii)Government-owned banking hjjjon the queue of adoption of AI POWERED SYSTEM to secure the internet banking.

iv)Nigerian commercial banks have data leaks, insecure shield compared to government owned banks which accounts for the lack of AI POWERED SYSTEM.

v) The banks rejected the adoption of AI in their banking system due to lack of technology to handle the algorithm involved.

4.5 Findings of the literature review.

The reviewed literatures support the use of AI for internet banking security and encourages its application to track down hackers. It showcased its faster responses on internet banking activities. However, it showed that AI has flaws that needs to be addressed for efficient use of it to combat internet banking. Here, table 4 shows the analysis of the five reviewed papers

S/n	**Authors and Date**	**Method used**	**Technology used**	**Research gaps**	**Security**
I	Chakraborty et al., (2022)	Quantitative analysis	No AI	No AI	Not achieved
II	Kumar et al., (2022)	Survey	No AI	No AI	Weak security
III	Juin et al., (2022)	PLS for analysis	AI powered	No-AI method	Partial security
IV	Kharm et al,	Quantitative analysis	No AI (Biometric)	Lack of AI powered system	Incomplete security achieved
V	Guptal et al,. (2023)	Data collection	AI used	AI used	Partial security

Table 4:

From the findings, it shows that AI is highly needed to be Adopted in the Nigerian banking sector to secure the system from threats and attacks.

4.6 Threats and challenges of AI development.

1. Data Breaches: Unauthorized access to sensitive data, compromising customer information and financial security which create huge losses.
2. Fraudulent Activities: AI-powered fraud detection must stay ahead of evolving tactics, such as phishing, malware, and identity theft and as well combat this menace.
3. Cyber Attacks: Protection against DDoS, SQL injection, and other attacks targeting online banking infrastructure.
4. AI Model Manipulation: Ensuring AI decision-making integrity, preventing bias and tampering.
5. Customer Education: Raising awareness about online banking security best practices.
6. Regulatory Compliance: Adhering to evolving regulations, such as GDPR and CCPA.
7. Ethical Considerations: Addressing concerns around AI-driven decision-making and potential biases.
8. Third-Party Risk Management: Ensuring security and compliance across the entire supply chain.

However, there are equally vulnerabilities that makes the internet banking and cybersecurity to be exposed to cyberattacks leading to damages, loss of information, data corruption and malfunctioning of information. Addressing these vulnerabilities is crucial to ensuring the security and reliability of Intelligent Shield and the overall integrity of Internet banking.

4.6.1 Vulnerabilities.

Here are the discovered vulnerabilities of Intelligent Shield of an AI-powered system for secure Internet banking:

1. Data Poisoning: Manipulation of training data to compromise AI decision-making.
2. Model Inversion Attacks: Reverse-engineering AI models to extract sensitive information.
3. Adversarial Attacks: Crafting inputs to deceive AI models, leading to fraudulent transactions.
4. Bias and Discrimination: AI decisions influenced by biased data or algorithms.
5. Overreliance on AI: Human oversight neglect, leading to unchecked AI errors.
6. Insider Threats: Authorized personnel manipulating AI systems for malicious purposes
7. API Vulnerabilities: Exploitation of API weaknesses, granting unauthorized access.
8. AI Model Obsolescence: Failure to update AI models, leaving them to new threats

Practical application of Artificial Intelligence (AI)

AI is expanding across various sectors, offering significant opportunities and addressing key challenges. Here are some insights based on recent literature from 2022 and onwards:

1.Economic Diversification and Growth:

AI is playing a crucial role in diversifying Nigeria's economy beyond its traditional reliance on oil. AI-driven innovations are fostering growth in agriculture, healthcare, and fintech, among other sectors. For example, AI-powered tools are enhancing agricultural productivity through predictive analytics and optimized crop management.

2. Healthcare Advancements: AI is transforming the healthcare sector in Nigeria by improving diagnostic accuracy, patient care, and access to medical services. AI-driven telemedicine and diagnostic tools are particularly beneficial for remote and underserved areas, helping bridge the healthcare gap

3. Fintech Innovations: Nigeria's burgeoning fintech industry is leveraging AI to enhance credit scoring, fraud detection, and personalized financial services. This has significantly increased financial inclusion, providing access to banking services for millions of Nigerians who were previously unbanked.

4. Education and E-Learning: AI applications in education are providing personalized learning experiences and virtual classroom settings. However, challenges such as poor internet connectivity and electricity shortages need to be addressed to fully realize the potential of AI in education.

5. Autonomous Vehicles and Transportation: The development of autonomous vehicles in Nigeria promises to reduce traffic accidents and improve transportation efficiency. AI technologies in these vehicles enable them to make intelligent decisions about navigation and safety. However, issues like car hacking and the need for robust network infrastructure pose challenges.

6. Regulatory Framework and Human Rights: The development of a comprehensive legal and regulatory framework for AI in Nigeria is essential to safeguard human rights, democracy, and the rule of law. The Nigerian government is working on policies that address the ethical use of AI, emphasizing the protection of human dignity and preventing misuse.

7. Counter-terrorism and Security: AI is being utilized in counter-terrorism efforts by analyzing patterns and simulating various scenarios to enhance security strategies. This application of AI helps in predicting and mitigating potential threats, thereby improving national security.

4.6.2 The development of an AI-powered system for secure banking, has the following limitations:

1. Data Quality and Bias: AI decisions are only as good as the data used to train the system, which may be biased or incomplete.

2. Overreliance on AI: Human oversight and judgment may be neglected, leading to unchecked AI errors.

3. Explainability and Transparency: AI decision-making processes may be difficult to understand and interpret.

4. Adversarial Attacks: AI systems can be vulnerable to targeted attacks designed to deceive or manipulate them.

6. Regulatory Compliance: AI systems must comply with evolving regulations, such as GDPR and CCPA.

8. Dependence on Third-Party Data

9. Lack of Human Intuition: AI systems may not replicate human intuition and judgment in complex situations.

Curbing these limitations are crucial to ensuring the effectiveness and reliability of Intelligent Shield and the overall security of banking systems through the use of AI.

5.0 Conclusion:

The results obtained from the structured questions of the six selected banks and its inherent traits assisted in the development of secured internet banking through the use of AI POWERED SYSTEM coupling intelligent shield. This was achieved through End-to-end Encryption, Firewalls and Intrusion Detection, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Regular Security Updates and Patching, Strong Password Policies, Monitoring and Incident Response, Customer Education, Two-Factor Authentication for Transactions, Regulatory Compliance, Penetration Testing and Vulnerability Assessments and Secure Internet Banking Platform. However, more are to be done in straightening the internet banking sector due the high level of evolvement of AI POWERED system.

5.1 RECOMMENDATIONS:

Based on the research and findings, there is need to adopt the following;

i)Adoption of AI POWERED SYSTEM for secure internet banking.

ii)Development of AI algorithm to secure the internet banking is needed.

iii)Regular security updates and patching of the intelligent shield.

ACKNOWLEDGEMENT:

This work acknowledges the input of Prof. Otavio Gomes of federal university, Itajuba, Brazil which was conceived in an Article project construction of class assignment on “EC343E; Introduction to cyber-Security”. His assessment and contribution were highly immeasurable.

REFERENCE

Ahmed, M., et al. (2021). Cybersecurity threats to internet banking: A systematic review. Journal of Information Security and Applications, 56, 102524.

Chakraborty, S., et al. (2022). Artificial intelligence in cybersecurity: A review of recent advances and challenges. IEEE Transactions on Neural Networks and Learning Systems, 33(1), 2022.

Jain, A., et al. (2022). Intelligent Shield: An AI-powered cybersecurity system for secure internet banking. International Journal of Advanced Computer Science and Applications, 13(2), 2022.

Kumar, R., et al. (2022). Internet banking security: A review of threats, vulnerabilities, and countermeasures. Journal of Banking and Finance Technology, 3(1), 2022. - *Raza, S. A., Salman, F., Zaidi, S. A. H., & Qazi, A. (2020). Artificial Intelligence in Banking Sector: Challenges and Opportunities. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). https://doi.org/10.1109/icccnt49239.2020.9225419*

- *Swathi, K., Reddy, K. R., & Bharathi, P. (2019). AI in Banking and Finance. 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). https://doi.org/10.1109/icecct.2019.8869224*

- *Jain, S., Gaur, S., & Singh, P. (2020). A Survey on Behavioral Biometrics for User Authentication in Mobile Banking. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). https://doi.org/10.1109/icccnt49239.2020.9225556*

-*Huang, K.-Y., & Rustogi, A. (2018). Deep Learning and Chatbots in Banking: A Guide to AI Applications. IBM Developer. https://developer.ibm.com/articles/cc-chatbot-banking-deep-learning-applications/*

- *Chuang, Y., Tsai, C.-F., Lin, Y., & Liao, W. (2020). Robotic Process Automation in Banking Sector: A Systematic Literature Review. 2020 IEEE 8th International Conference on Applied System Innovation (ICASI). https://doi.org/10.1109/icasi50041.2020.9249956*

- Nami, M. R., Alizadeh, M., & Shabani, H. (2020). Banking with artificial intelligence: Challenges and future directions. Journal of Retailing and Consumer Services, 53, 101736. https://doi.org/10.1016/j.jretconser.2019.101736

- Biggio, B., Nelson, B., & Laskov, P. (2018). Poisoning Attacks against Support Vector Machines. arXiv preprint arXiv:1206.6389.

- Dastin, J. (2021). Amazon hit with lawsuit alleging discrimination in AI hiring tool. Reuters. https://www.reuters.com/technology/amazon-hit-with-lawsuit-alleging-discrimination-ai-hiring-tool-2021-09-14/

- Fatima, M. T., Yan, B., Kiani, S. L., & Wang, Y. (2021). AI in Banking: Opportunities, Challenges, and Outlook. IEEE Transactions on Intelligent Systems. https://doi.org/10.1109/tii.2021.3126656

- Kshetri, N. (2019). Cybersecurity challenges and the role of artificial intelligence in modern banks. Journal of Retailing and Consumer Services, 51, 72-83. https://doi.org/10.1016/j.jretconser.2019.05.016 *Literature Review: AI Cyber Protection in the Banking Sector*

- Vatanparvar, K., Jafarzadeh, H., & Dehghantanha, A. (2020). Deep Learning-based Cybersecurity Solutions for Banking Systems: A Survey. IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/tii.2020.2979655

- Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. (2019). Behavioral Biometrics in Cybersecurity: A State of the Art Survey. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/comst.2019.2894092

- Liu, Y., Ning, H., Wang, Y., Yang, C., Zhang, L., & Zhang, Y. (2021). Fraud detection for banking industry based on artificial intelligence: A comprehensive review. Expert Systems with Applications. https://doi.org/10.1016/j.eswa.2021.115205

- Sharma, S., Jain, D., & Singh, S. (2020). AI-based Cybersecurity Framework for Banking Sector. 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). https://doi.org/10.1109/aisp50998.2020.9244793

-P. Tayal, N. Rastogi, T. K. Ahuja, S. Tyagi, K. Joshi and Y. M. Mohialden, "Impact Of Ai On The Banking Industry 4.0," 2022 7th International Conference on Computing, Communication and Security (ICCCS), Seoul, Korea, Republic of, 2022, pp. 1-4, Doi: 10.1109/ICCCS55188.2022.10079399.

-C. Sachdeva, V. P. Gangwar, V. Grover and S. Gochhait, "Cognitive Dissonance in Banking Employees: Exploring Factors Amid the Artificial Intelligence Revolution," 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS),Manama,Bahrain,2024,pp.17311735, doi:10.1109/ICETSIS61505.2024.10459558.

-H. M. Alzoubi et al., "Cyber Security Threats on Digital Banking," 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, 2022, pp. 1-4, doi: 10.1109/ICAIC53980.2022.9896966.

-H. U. Khan, M. Z. Malik, S. Nazir and F. Khan, "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," in IEEE Access, vol. 11, pp. 80181-80198, 2023, Doi: 10.1109/ACCESS.2023.3298824.

-G. ALMahadin, P. D. Sawant, S. Ali, A. Anjum, S. K. Ibrahim and S. J. Naser, "Enabling Smart Banking AI and IoT: Challenges and Opportunities," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2023, pp. 1-6, Doi: 10.1109/ICSES60034.2023.10465372.

-S. Gopal, P. Gupta and A. Minocha, "Advancements in Fin-Tech and Security Challenges of Banking Industry," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6, Doi: 10.1109/ICIEM59379.2023.10165876.

-R. Pratap Singh Chauhan, S. K. Sonker, M. Kaur, C. Sharma, R. Singh and R. Singh, "Optimizing IoT Threat Mitigation with Artificial Intelligence in Banking: A Multi-Objective Approach," 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2024, pp. 296-301, doi:10.1109/ICDT61202.2024.1048961

-Rania Elouidani, (2023) ‘‘artificial intelligence technologies in companies: case of the banking sector in Morocco” 8(3):216-237

DOI:10.48375/IMIST.PRSM/remses-v8i3.36998