European Journal of Engineering and Technology Research
Vol 8 | Issue 5 | October 2023
ISSN 2736-576X

RESEARCH ARTICLE

A Graphical and Qualitative Review of Literature on AI-based Cyber-Threat Intelligence (CTI) in Banking Sector

Eke Roberts Ndukwe[1,*] and Barilee Baridam[2]

ABSTRACT

Cyber threats have become a threat to the banking industry, and resulting in the business attempting to implement artificial intelligence strategies while build resilient cyber-defense systems. This is done to ensure that unauthorized access, which leads to cyber-attacks, is severely limited. The credit trade is undergoing significant technical change. Because of this, crucial to comprehend implications a cyber threat, as well as how technologies implementation that is artificial intelligence will revolutionize entire sector. Paper aims at examining how AI affects cyber threat intelligence in the commerce subdivision. A graphical and qualitative analysis of available publications, primarily conference papers, was carried out. Despite being widely used in India and the United States, there are still few studies in the AI field. Furthermore, no study found that African banks used AI for cyber threat intelligence.

Keywords: Artificial intelligence (AI), Banking sector, Cyber-threat intelligence, Graphical & Qualitative analysis.

Submitted: August 31, 2023

Published: October 18, 2023

10.24018/ejeng.2023.8.5.3103

[1] *Information Systems Engineering, Center of Information & Communication Technology, Faculty of Engineering, University of Port Harcourt, Nigeria.*
[2] *Computer Science Department, Faculty of Computing, University of Port Harcourt, Nigeria.*

* ***Corresponding Author:***
e-mail: ekenroberts@gmail.com

1. Introduction

The latest developments in cyber threat intelligence have caught the interest of academics and organizations. Cyber threat intelligence is not brand-new; it has been crucial to preserving safety within networks for quite some time as systems have been in existence and able to interact. According to Gartner, threat intelligence is information, which can be utilized to guide decisions about how to respond to an ongoing or developing threat or harm to assets; includes context, structures, indications, adverse effects, and guidance that can be taken immediately [1]. Following this definition, it becomes clear that the fundamental underlying reality is that of evidence-based knowledge because CTI must be supported by evidence in order to be trusted. Furthermore, it is essential that the knowledge in question be actionable and able to be exploited to thwart threats. The emphasis of CTI includes the motivations, objectives, and capabilities of the enemy [2]. An eye to fulfill the demands of prevalent defensive tactics that deal with and respond to cyber-attacks, intelligence must be actionable and not just data. Intelligence may be considered as the information and knowledge gathered about an adversary through observation and analysis.

According to [3], there is a rising need to collect more threat intelligence, yet doing so successfully presents a difficulty. As shown in Fig. 1, there is a connection between intelligence, data, and information. To get the most out of a threat intelligence platform and cybersecurity, it is essential to comprehend the vast differences between noise, threat data, information, and intelligence as reported by [4]. Data consists of essential, unexpurgated and basically unfiltered evidence characteristically offered as impressions from pointers and cyphers. The basic blocks of communication are words (vocal and/or transcribed), records, illustrations, and representations (tranquil or alternatively moving), whereas signals are instrument and/or aural readings of contact, lightbeams, sound, aroma and flavour. From a professional standpoint, [5] defines intelligence as data that has been enhanced, evaluated, and processed, and the result must be useful, relevant, and actionable. Through rational and analytical process conduct, anyone who can give contextual data and provide usable output can meet those three standards.

Terms "cyber-threat" likewise "cyber-attack", which are the most frequently used in debates, have multiple definitions. The US government gave a broad definition of a

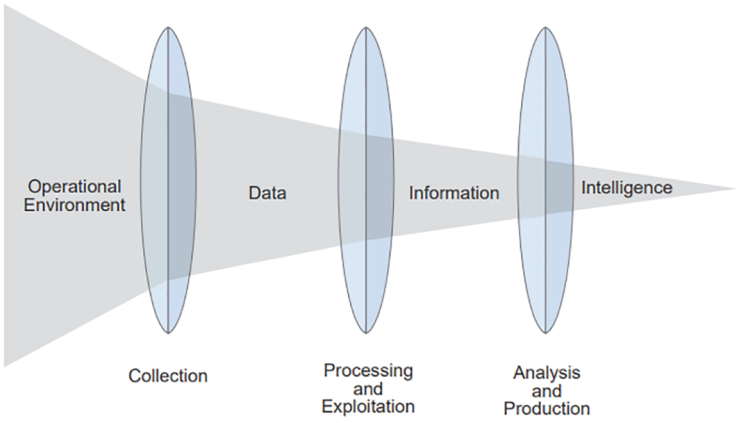

Fig. 1. Information, data & intelligence association [6].

cyber-threat in 2013 that incorporates several security precautions: "Cyber-threats" refer to a extensive assortment of harmful actions that may occur in cyberspace [7]. Dangerous viruses, theft of patents, defacing web pages, and covert operations constitutes uncommon elements of these risks. The wordlist delineates cyber-threat "the likelihood that someone will attempt damaging or ruin a computer grid, computer system, website by covertly changing information on it without authorization" or "the likelihood of a mischievous crack in impairment or dislocate network", unlike the Government of US definition [8], [9]. The act of attempting to harm, obliterate a computer structure network, or website furtively modifying the information contained therein without authorization is known as a cyber-attack [9]. There are commonly four methods of intrusion detection: anomaly, abuse, specification-based detection, and stateful protocol inspection [10], [11].

The first step in anomaly-based detection techniques is to identify the subject's typical actions, which could be that of a human being or a system. Whenever an act departs considerably from the customary course of conduct or routine, it is regarded as unusual, disruptive, or intrusive. As the system of identification tries to develop an understanding of typical network traffic, anomaly detection's primary goal is to discover novel assaults, with whatever deed departs from the normality profile being flagged as extremely problematic. The network communication is scanned by this intrusion detection system for information that is incorrect, unenforceable, or unusual in any other way. False discoveries and erroneous negatives are two distinct scenarios that could happen in anomaly detection. False positives are ambiguous patterns that are marked as invasive yet do not obtrude, and false rejections are abnormal responses designated as inconspicuous but actually are. Consequently, this technique has the drawback of producing an unwarranted quantity of pseudo positives and denials. The biggest plus or benefit of anomaly detection is that it can discover unidentified assaults. Anomaly spotting methodologies include data extraction, advanced statistical estimation, machine learning, and embedded Markov algorithms [12].

Misuse detection searches for distinct patterns (such as signatures, regulations, actions, or routines) in the gathered network data in order to recognize DDoS incursion types that have been beforehand identified or recognized assaults. These detection methods frequently have low false alert rates and high recognition rates. On the contrary side, a misused tracking strategy misses unidentified DDoS attack types. Approaches for pattern matching are widely used in misuse detection [13].

Instead of acquiring a normal description of the operation, specification-based surveillance establishes normative conduct and marks anything that diverges as invasive. This technique's drawback is that it can be difficult to define and validate behavior for platforms with numerous different parts and applications.

Similar to anomaly-based detection, stateful protocol inspection can analyze traffic at the layers of network and transport, alongside exclusive to particular traffic at the application level, which anomaly-based detection is unable to do.

1.1. Methodologies Deployed in Detection of Cyber Threat

IDSs are never completely accurate in their detection; they frequently generate false positives (confusing positive behavior for negative behavior) and false negatives (failure to recognize fraudulent conduct). In order to identify false positives from actual hostile actions, many firms prefer to modify IDSs to decrease false negatives while raising false positives. The majority of IDSs also have the ability to counteract common evasion techniques, like altering the timing or format of malicious activity to modify only its look but not its impact in order to avoid detection by IDSs. Most IDSs use several detection methods either independently or jointly, to provide more thorough and precise detection. According to [11], the most common categories of detection techniques are:

Signature-based, which locates instances by contrasting recognized danger signatures with recorded events. This is very efficient at identifying vulnerabilities that are already known, but it's not quite as successful at identifying attacks that aren't established to be threats and many variants with identified dangers. The majority of multi-event assaults are incapable of being detected by signature-based detection considering it is unable to comprehend and track complex communications.

For the purpose of identifying significant alterations, anomaly-based detection relates ideas regarding what characterizes standard conduct to real incidents. This

tactic employs the recourse to forms that were built by monitoring the characteristics of routine behavior over time. The IDPS subsequently matches the traits of the present activity to profile-related parameters. Approaches that use anomaly-based detection can be very successful at finding threats that were originally undetected. Common issues with anomaly-centered monitoring include the accidental inclusion of criminal acts within a record, the creation of profiles that are insufficiently complex to reflect actual computing exercise, and the production of a large number of false positives.

Stateful protocol analysis juxtaposes genuine events to predefined profiles of acceptable protocol action that are widely accepted descriptions of each standard state in order to find discrepancies. The method counts on supplier-created uniform standards specifying ways different techniques may and should not be employed, contrary to discovery on anomaly using host, conversely characteristics-precise configurations. Through a notion of state, it is capable of understanding and monitoring the status of protocols, which enables it to recognize a variety of violations that alternative methods are not equipped. Stateful protocol analysis has a number of disadvantages, such as the difficulty in building very accurate representations of protocols, the substantial enterprise prerequisites, and the incapacity to identify exploits that do not go against the fundamental principles of widely tolerable rules practice.

1.2. Cyber Threat Detection Location

IDS may be additionally categorized based on where it is deployed. These categories are predicated on victim-end, source-end, or intermediate mechanisms. (a) The routing devices of the target network frequently have a DDoS detection function implemented at the victim end. The prevention software monitors known intrusion signals as well as routine activity rhythms. The processing components refresh this knowledge as it evolves into been available. Modifications are made to the saved infiltration signatures and procedures for other important events, including erroneous alerts. The manipulation portion is responsible for routinely. recording formation data, containing the results produced at intermediary steps. Since it has more opportunities for investigating the flow of traffic, a victim-end diagnosis scheme is usually successful to offer greater recognition performance than comparable techniques at the compromise of heightened resource depletion. One major drawback lies in the fact such technologies primarily detect attacks once they have hit the target, which could be an accentuation victory if actual clients have experienced liability. An effective defense against DDoS assaults cannot be provided by a victim-end preventive strategy when the volume of traffic being targeted is exceptionally large.

Source-end – Through screening hostile traffic in advance before it mixes with the rest of attack communication moving within the network's boundaries, assault activity can be blocked ahead of hitting the network being targeted and conflicts may be averted. Additionally, this mitigation not exclusively facilitates verification easy, but it also enables outstanding detection exactitude owing to minimum network traffic flow accumulation at the originating endpoint. Because of this, the primary benefit of source-end alerting for DDoS attacks is that it has the potential to safeguard the networks at the site of offensive fabrication, lowering the risk that the network being attacked will suffer catastrophic harm. This recognition method does, however, have a significant weakness because, during an assault, strike origins are recurrently dispersed and an individual source acts very similarly to regular traffic.

The constraints of DDoS victim-end and source-end detection may be solved by an intermediate network security by coordinating the challenges of attack exposure correctness and frequency use. An important concern is how quickly such a defensive system can be deployed. Use the detecting system of overall Internet gateways to get best detection accuracy possible since if this scheme isn't available on some routers, the detection and traceback activities might not succeed. Because all Internet routers must be reconfigured, full adoption of this method is therefore practically unattainable.

1.3. Infrastructure Used in Cyber Threat Detection

Network-based intrusion detection is a particular kind of IDS which analyzes network traffic in order to detect unusual behavior across the OSI model's layers and determine its purpose. It notices packets of data, examines them for abuses or oddities using network traffic data from the router's memory or saved network traces. Host-based intrusion detection systems scrutinize network traffic as well as system-definite factors like program calls, regional security regulations, regional log audits, and more. Each machine needs to have a HIDS installed and set up specifically for that program and functioning mechanism. Host-Based, which keeps an eye on a particular host's attributes and the happenings that take place on that host, searches for inappropriate behavior. In accordance with the data provider, there are two categories for the host-based intrusion identification structure. Reference [11]:

-Implementation employing HIDS—Mentioned IDS category accepts data as request format, for instance logging files generated by barriers, database control tool, or web servers, the layer application is where this technique's weakness lies.

-The HIDS Based Host—This type of IDS gets data pertaining to the operation of the watched machine. Sometimes, this data takes the shape of software investigation trails. Along with the details of the component structure which aren't examined in a typical assessment of the computer's operating system and tracking techniques, it could additionally involve the records framework of other logs produced by working system operations. The aforementioned may additionally employ the information provided by a different dependent implementation IDS.

Hybrid intrusion detection [14]—To improve adaptability and safety these platforms employ both host-centered and configuration-based detection of breaches. These systems often possess complicated attributes that can be changed according to the needs in relation to traffic statistics, IDS assignment, and notification style.

1.4. Intrusion Prevention Systems

DDoS is a coordinated effort, making it challenging to pinpoint the source of an attack in real time. Preventative measures are designed to either totally eliminate the possibility of DDoS assaults or to give potential victims the ability to survive the onslaught without restricting access to services for legitimate customers. Focusing on inline technology is known as an IPS, working on real-time detection and blocking of hostile network activities. An Intrusion Prevention System is any piece of either software or hardware, which possesses the capacity to detect, counter established and mysterious dangers. This scheme is essentially a firewall that can spot irregularities in network traffic and then stop potentially risky activities. Many DDoS avoidance techniques have been created [15], [16].

2. Overview of Cyber Threat in Developing and Developed Countries in Banking Sector

In accordance with the study's problem and its stated goal, overview of contemporary and associated scholarship is provided this subsection. To demonstrate why a review of earlier studies is necessary, an evaluation of those studies is made [17] when examining how clients regarded financial institutions offerings, concentrated on the post-demonetization stage. It was revealed that customers had significant problems adopting facilities provided and that termination had significantly changed their perceptions of banking and fiscal services. Additionally, acknowledged is part of main troubles the Indian banking system now experiencing is irrecoverable assets. Reference [18] evaluated growth of online bank benefits, consumer facilities' existence understanding prior demonetization, and governmental creativities for e-services usage. The scrutiny came to conclusion that the banks undertook intentional endeavors to inform its clientele throughout the pre-demonetization era regarding new-fangled mediums via talks, workshops, etc., Individuals are progressively more concerned with safekeeping and confidentiality matters after becoming accustomed to electronic financing operations. According to research conducted by [19], Jordanian commercial banks must concentrate on concealment and protection issues given the rising risk of cyber vulnerability. The financial service sector is anticipated to be equipped with guarantee measures designed to secure clients' sensitive information because the worldwide web is a transnational ecosystem that is susceptible to illegitimate infiltration and exploitation. In order successfully compete with other banks, banking services are being updated as a countermeasure to computer crime as well as satisfy the vibrant environment of shifting client wants, also inclinations. Tasking is what customers want from banks, especially in terms of rapidity, safeguard, and accuracy. To gain competitive edge by growing their customer base, luring prospective clients, and retaining their existing clientele, businesses within this domain are continually introducing innovation and cutting-edge approaches to satisfy quality and customer expectations. Through [20], effort was undertaken to examine how customers in Kenya perceived smart banking. Contrasting established economies, particularly where emphasized as key criteria for the widespread utilization of unfixed banking options, the superseding demographically traits and consumer stances may have an entirely different effect on the developing market. The investigation also revealed that there were no gender-based differences in respondents' preferences motivated simplicity besides danger of utilizing web banking. Reference [21] study also found digital crimes negative impact in respect effectiveness and credibility of Pakistani banks. The outcomes further indicate the regime's actions generally mitigate the effects of cybercrimes substantially. This survey was unable to identify, however, whether the aspect of Pakistan's banking industry's productivity was genuinely damaged by cybercriminals. Reference [22] found although 31% of those surveyed merely acknowledged knowledge of various types of cyber hazards listed when looking at the impact of those dangers concerning customer's attitude utilizing virtual transactions provisions. The implication is over seventy percent of the patrons of the internet had no understanding of the risks presented. This unfamiliarity among wired users may be ascribed to low levels awareness plus poor sensitization across entirely dependent chunks. Malicious hackers' profit from amateurishness as a gate to the information of unguarded clients in order to commit fraud and other crimes. Additionally, more than 60 percent customers couldn't recognize nor effectively handle communication protect issues. The precautions that should be taken when using online banking services were also unknown to roughly 55% of the users. This creates a requirement for banks to update their knowledge of the usage, securing using the internet for banking and transmit that knowledge unto their consumers through appropriate sensitization. To reduce the organization's loss from cyber-related crimes, prevention and detection costs are incurred. The introduction of reactive techniques to address the detected incidents of cybercrime results in response costs (such as disaster recovery response cost). Online transfers or full account takeovers used to launder stolen money have an impact on bank finances. This can also entail sowing doubts about the financial institution's dependability and safety. The potential cost associated with a cyberthreat can be recognized in indirect expenses or image-related costs [23]. Fig. 2 illustrates the cost classification of finance business cyberthreats influence.

2.1. Cyber Threat and Its Impact

Cybersecurity, espionage menace committed by sophisticated crooks; constitutes one of the greatest grave and puzzling complications afflicting numerous business establishments. Basically, encompasses unlawful entry to private or sensitive corporate information used for selfish purposes. This occurs across the internet and other forms of exchange of data anywhere a computer connection to cyberspace is present [25]. According to [26], cybercrime forms felonious act performed in the online world, supplementary e-mail and information channels. Focusing on this, [27] stated that internet misdemeanor implies "cyberspace-related offenses thru electronically induced media". Cyber intrusions comprise authentic gathering

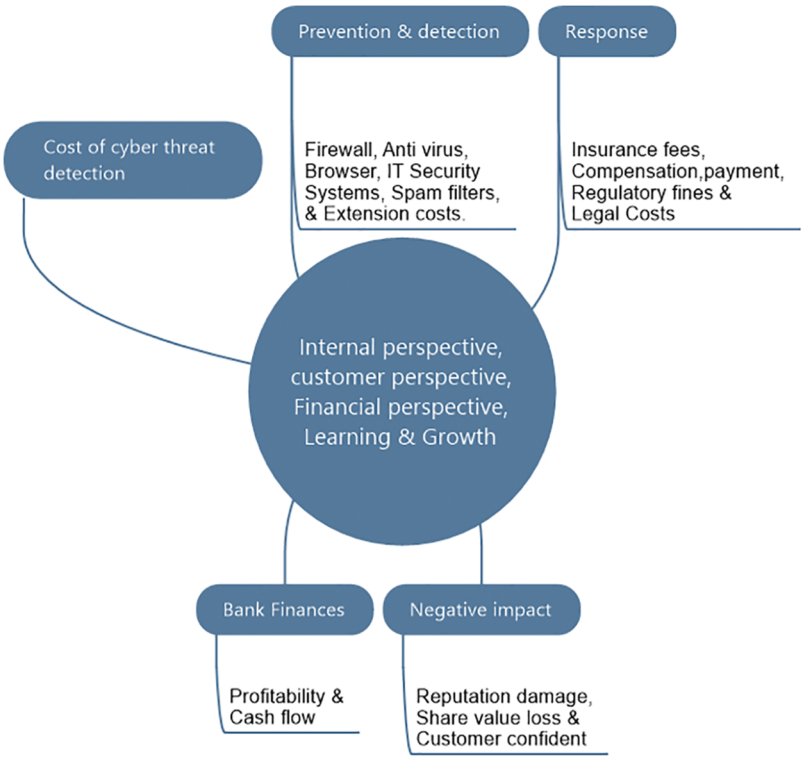

Fig. 2. Rate cataloguing of banking sector cyber threat consequence [24].

of evidence and interactions that make use of powerful criminological and exploratory tools and are carried out swiftly and precisely by the Nigerian inter-banks' mediation mechanisms, and (USD 2.5 billion) NGN 413 billion as stated by new Horizons Limited, an ICT firm Nigeria domiciled [28], [29]. Whereas such expenditures may stay computed, the value of human misery albeit catastrophe is unfathomable, and it currently amounts to greater than an actual lawbreaking [30]. For the sake of safety cum financial stability of any republic, it becomes essential to reinforce cyber defenses, also shield delicate information. There is a need to address the issue for the security of the firm and its stakeholders as malware has recently become a major menace to all companies worldwide. The hack ultimately had a negative effect on the impacted companies' aggregate valuations and profitability per capita [31]. In this section, past studies have revealed that research on cyber security in banking is still ongoing in Nigeria. However, no study has shown that AI has been applied on cyber threat perspicacity crosswise banking trades of Nigeria.

2.2. *Nigerian Banking Internet Safety*

New and significant threats are present at environment of broadcasting and informational technology as it develops. Cyberattacks can now seriously affect society in novel and important ways. A few instances of numerous daily large-scale crimes linked to computers committed are online fraud and cyberattacks [32]. Foreign investors have been considerably discouraged by these offenses, which has long tarnished the credibility of Nigeria overseas. Central Bank of Nigeria's quest toward cash free culture per the unprecedented rise in mobile connectedness have backed the advance of cybercrime. Reference [33] claims that monetary burden of 'cyber-attacks' is extensively high and escalating swiftly. Nigerian banks forfeited Naira 159 billion for cybercrime within 2000 & 2013, in accordance with account released.

3. Artificial Intelligence

Understanding the connections between Artificial intelligence, Machine learning, joining Deep learning may be challenging. Aforesaid development affecting artificial intelligence (AI), a comparatively recent phenomenon, began during latter section of the 20th century. But with ancient Greek, Egyptian tradition, the idea that man-made statues might be intelligent and emotional is depicted [34]. A workshop held in 1956 at Dartmouth College is often cited as the catalyst for AI research. At this conference, axiom "artificial intelligence" was created courtesy John McCarthy and Marvin Minsky distinguish it from related disciplines comparable to cybernetics [35]. By this time, AI had advanced to the stage where it was even capable of speaking English and resolving algebraic problems. Latter semi part of 1960s, the US Department of Defense had significantly increased funding for AI research owing to the positivity of the period [36].

Unfortunately, the initial enthusiasm for this novel science did not endure, also during the 1970s, interest in AI technology began to wane. In the 1980s, the development of artificial intelligence technology saw a brief surge. Nevertheless, some recent breakthroughs in technology in the late 1980s were not practical or profitable; so, this revival was only momentary. This marked the start of a second break in AI research [36]. Another renaissance in AI technology occurred in the belatedly 1990s and beginning of 2000s. This period saw the development of

numerous applications for AI, such as medical diagnostics, logistics, and data mining [37]. In a sense, artificial intelligence (AI) is a contemporary technical discipline that investigates and develops concepts, approaches, tools, and applications to mimic, supplement, and enhance intellect of people [38]. An offshoot of computer discipline aims to comprehend fundamentals of brainpower while developing different types of brainy machines that act like people. This discipline includes research in the fields of native tongue processing, specialist systems, automation, and visual analysis. AI is able to replicate the information flow that powers human intellect and perception. AI has the potential to outperform human intelligence even though it does not yet match it. Being capable of creating completely self-aware entities who collaborate alongside the surroundings in order to discover the most effective behaviors and hone them over the course of time by means of experimentation and learning represents a few of the goals of the study of artificial intelligence (AI). It has taken a while to develop AI systems that are responsive and learn very well. This encompasses the field of robotics where machines can perceive their environment and respond to it. Software-based elements known to be able to engage with audiovisual and natural language are primarily included in this.

4. Utilizing AI in Banking Market Cyber Threats Combat

Definite rise in AI-driven cyberattacks suggests AI potential to both refine and undermine cybersecurity. Nonetheless, because they are unforeseen (such as in the banking sector, for example), employing artificial intelligence in critical managements presents a number of challenges. The majority of these concerns center on matters of security, reliability, correctness, and dependability. The main criteria establishing those cyber-security solutions' extent of reliability is how well they are guarded against distinct cyber-attacks. By implementing a powerful cyber protection system, one can increase client confidence and the potential of using banking products and services [39]. Artificial intelligence (AI), catch-all expression for variability of practices and blueprints calculated to reduplicate intricate abilities, like making decisions independently and utilization of language [40]. Machine Learning's ambition is picture similarities data inherent and make well-versed judgments. Based on system explicitly informed veracious reactions, supervised and unsupervised learning can be differentiated in machine learning [41]. Artificial neural networks are exerted in Deep learning to apprehend extremely knotty information. In the field of banking, AI assists the employment of state-of-the-art analytical instruments and imaginative marketable solutions. Banks offer channelized habitué accessibility, learn about consumer habits, and tailor offerings adequate client needs recognitions to AI-powered know-hows [42], [43]. With rise of FinTech companies, the world of finance is now more competing. The expectation is that banks will deploy imaginative strategies and suitable precautions for safety to protect their customers' information while also meeting their customers' needs [44]. However, comparing incumbent banks against emerging FinTech companies, established institutions are clearly distinct handicap with regard to leveraging advances in technology [43]. Consequential of outdated procedures impeding the acceptance of modern technologies, banks may find it difficult to change. Because creative options cannot be used with antiquated finance and protection software platforms, this may pose additional security risks. Data privacy is foremost concern encircling banking field AI deployment [45]. Since the development of corresponding rules and regulations is in the works, yet unclear financial institutions ought to depend on outside service outfitters to maintain data privacy [40]. Integrating resources with AI to analyze employee and customer communication, like normal linguistic processing, or chat bots interacting with punters, might encroach onto individuals' secrecy [41]. The terrain of regulations continues to be changing. This ambiguity could make it more difficult for banks to combat risks associated with cybersecurity. As a result, the current paper uses graphical and qualitative review methods investigating bearing of AI-based Cyber Threat Intelligence (CTI) in banking sector publications. Through organized screening and synthesis of research data from core investigations, a qualitative systematic examination gathers findings regarding a particular subject.

5. Results

The current study makes recourse to meta-analysis to evaluate application of AI for defense in Nigeria's banking system. This enables investigation into the nation's current AI processes grounded on the opinions and practical knowledge of industry professionals. Search queries or protocol has been prepared following past works and keywords. Search queries: "cyber AND threat AND intelligence AND model", "cyber AND threat AND intelligence AND model AND in AND financial AND institutions", "cyber AND threat AND intelligence AND model AND in AND banking AND sector", "cyber AND threat AND intelligence AND in AND in AND banking AND sector", "application AND of AND ai AND in AND cyber AND threat AND intelligence", "application AND of AND machine AND learning AND in AND cyber AND threat AND intelligence". Date: 10th November, 2022. Source: https://www.scopus.com/results/results.uri?sort=plf-f&src=s&st1=CYBER+THREAT+INTELLIGENCE+IN+THE+BANKING+SECTOR&sid=d9ea1ed172fe50bdeb0e020750fbc5b1&sot=b&sdt=b&sl=62&s=TITLE-ABS-KEY%28application+AND+of+AND+cyber+AND+threat+AND+intelligence+AND+model+AND+in+AND+banking+AND+sector%29&origin=searchbasic&editSaveSearch=&sessionSearchId=d9ea1ed172fe50bdeb0e020750fbc5b1&limit=10

The dataset obtained from Scopus Database, ResearchGate, Google Scholar will be analyzed using VOS viewer.

Although, graphical reviews were created to convey knowledge in a compelling illustration of the level of research on applications artificial intelligence (AI) in cyber threat uncovering in banking sector studies. This review work employed Excel, VOS viewer and Mindjet mind

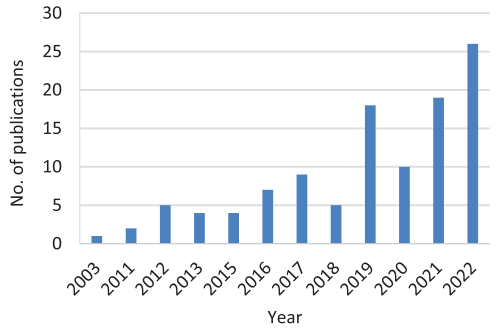

Fig. 3. Publication trend of "applications of artificial intelligence on cyber threat detection in banks" from 2003–2022.

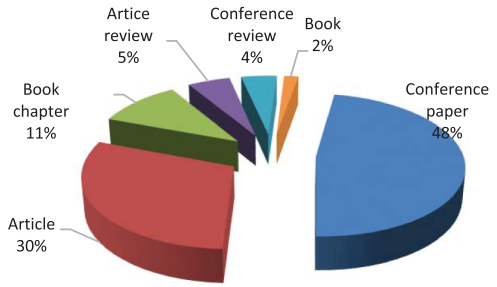

Fig. 4. Document types obtained from dataset.

manager software for graphical analysis. Meanwhile, the qualitative analysis was implemented in Excel 2019.

6. Results

Graphical review and qualitative analyses on the dataset containing, book chapters, journals articles and conference papers between 2003 and 2022 are presented in research trend order in Figs. 3 and 4. However, it can be seen in Fig. 4 that the publications contained more of conference papers (48%), followed by journal articles of amounting to 30%. It was observed that publication on AI application cyber threat revealing in sector of banking started from 2003 with a gradual increase until 2019 where the research interest increased rapidly till 2022. Therefore, it can be deduced that there is still interest in the research topic.

6.1. Keywords Used in AI-Based Cyber Threat Intelligence in Banking Sector Publications

The keywords used in AI based cyber threat detection also known as cyber threat intelligence (CTI) were analyzed, to determine the number of incidences and their tally link intensity (Table I). The by-word that appears most universally is "artificial intelligence" 52 (27%) in green color of the total followed by "machine learning" 39 (20%) and "cyber security" (20%), "cyber threat intelligence" is 8 (4%) out of the total.

From Table I it can be seen that the AI methods widely used in this subject area is machine, internet of things and deep learning whereas the type of threat that appear most is intrusion detection.

6.2. Countries and Publication Citations

The countries that have published real-world AI applicability in cyber threat. intelligence in banking sector

TABLE I: Authors Buzzwords & Link Strength

Keyword	Occurrences	%Occurrence	Total link strength
Artificial intelligence	52	27	78
Machine learning	39	20	62
Cybersecurity	39	20	35
Internet of things	12	6	23
Security	12	6	15
Deep learning	10	5	27
AI	8	4	8
Cyber threat intelligence	8	4	11
Intrusion detection	7	4	20
Artificial intelligence (AI)	6	3	2

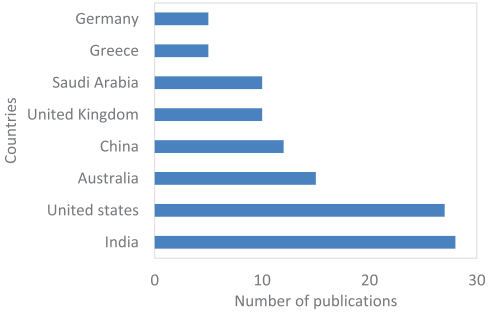

Fig. 5. The countries and their number of publications on "application of AI on cyber threat intelligence in banking sector publications".

arranged in the rank order of highest to lowest documents as well as number of citations. Here it shows that India has the highest number of publications amounting to 28 (25%) documents with 183 citations, followed by the United States with 27 (24%) of total publications. It can be deduced that India has more impact on the subject area. However, the countries that have published works in this area include India, United states, Australia, China, United Kingdom, Saudi Arabia, Greece and Germany (Fig. 5). The colors in the tables indicates that the range of publications, citations and total link strength. The countries publication and number of citations noted in below table.

6.3. Most Frequently Occurring Words in Publications Based on Word Cloud

Results are obtainable as a word cluster after using dataset determined on syllable patterns [46]. Word clouds parade furthermost happening texts passim analysis [47]. Giving qualitative assessments present study, "security" is the most popular wording cybersecurity researchers cited. Distinctively "information" and "banking" were second record emergence in published articles sourced from Results obtainable as a word cluster after using a dataset determined on syllable patterns [46]. Word clouds parade furthermost happening texts passim analysis [47]. Giving qualitative assessments present study, "security" is the most popular wording cybersecurity researchers cited. Distinctively "information" and "banking" were second record emergence in published articles sourced from Scopus. In terms of countries where the study existed, "India"

TABLE II: Countries and Citations

Nation-state	Publications	%Publication	Citations	Total link strength
India	28	25	146	273
United states	27	24	183	528
Australia	15	13	167	520
China	12	11	22	170
United Kingdom	10	9	91	354
Saudi Arabia	10	9	48	428
Greece	5	4	18	41
Germany	5	4	8	90

Fig. 6. Word cloud of most frequently occurring words in AI-based CTI on banking sector publications.

and "Bangladesh" all in Asian continent appeared significantly which corroborates the outcome of "keywords" and qualitative analysis in previous sections. Consequently, countries in Africa did not appear in the word cloud or in keyword analysis, which indicates that no research have shown that banks in Africa apply AI in cyber threat intelligence. The term "artificial intelligence" is the final, typically used phrase in the investigation, acting as the review main focus. The word cloud is presented.

6.4. Review of Related Works

Artificial intelligence shrinks opex, and improves customer assistance, and automotive proceedings. By digitizing knowledge workers, AI not merely gives banks more power, nevertheless renders its whole automation method sufficiently intelligent to handle rivalry and cyber hazards. Is constantly evolving, becoming more ground-breaking. AI is a critical component of bank's schemes and regimens. Enables financial institutions to more effectively combine anthropological and material resources to increase functioning and financial efficiency while also providing custom-built servicing. Foregoing advantages are no longer seen as possible prospects for banks. Leaders in the banking sector previously engaged in the necessary steps benefit from AI by embracing it. Moreover, AI provides the ability to predict future events scrutinizing antique behavior. One of standout eccentricities is that bankers employ these well-coordinated systems to make tactical decisions. These systems respond and anticipate like a human connoisseur and offer outstanding retorts braced on information that can be found instantly. These structures accomplish knowledge databases, which serve as archives for expert data [2]. Based on preceding relationships, AI gains greater insight into usagers and their comportments. Blending individualized services with honest dialogue, enables banks to provide financial resources, delivering results while encouraging significant client involvement and enduring associations [3]. Direct communication: Chatbots answer as logically as they can after identifying situations and emotions in messages. These logical tools encourage banks to work more efficiently and with less wasted time, enabling banks to conserve huge money sums, which adds up to overall savings that are worthwhile [4]. AI can perform fraud control by identifying questionable data patterns within a wealth of information. AI has previously studied the future behavior of data points using its own very skilled pilots. Effective cross-promoting, increased revenue boosted for banks [5]. A methodical process Self-regulating: With the help of this facility, numerous data-intensive, pricey, unreliable aids, resembling claim governance, can be self-regulated.

AI discovers hidden functions and saves banks millions of dollars due to capability of machine learning and cognitive. These cyberthreats affect not only bank accounts or sales accounts, but also money held by businesses in their business bank accounts as well as money controlled by banks. This details the dangers to financial organizations' operations and creditworthiness. Hence, the majority of banks have a knack for identifying and apprehending offenders. Since familiarity level, machine learning progress required in such skills entails more sophisticated whereby at the moment, illustrious technology type, such as AI, still hardly at all produced. This is due to the fact that using AI to compromise security is not really threaten cyber threats that produce viruses using such technology and may withstand sustained attacks if hackers were actively project participants. Or, at the very least, banks are aware that this is the case and do not fund AI security research because they believe that this will be the case in the future. There is no reason to defend against a threat if none exists. Artificial intelligence's role in preventing cyberattacks on banks [48]. In order to commit more crimes online, criminals are employing more and more cyberspaces equally developing info technology. Banks withal financial firms aim to use mode to reduce these cyber and linked dangers. AI technologies gifts a selection of opportunities that support the investment industry's wealth and development growth. With the ability to analyze a wide range of issues from a human perspective, artificial intelligence developed on the idea mimicking the humanoid psyche. Important concerns regarding information security, privateness are striking by expansion when using the internet and complicated dissemination. The banking sector has long utilized artificial intelligence.

However, banks have advanced significantly in their use of incorporated AI technologies. The banks numbers embracing AI actually rising, however, there is a risk of error due to AI capacity in dealing conventional jobs, both times. Banks, and other financial providers quickly adopting artificial intelligence so reexamine reasoning and

TABLE III: Summary of AI Techniques Used in CTI in the Banking Sector

Title	Accuracy	AI technique	Country	References
”Application of AI and its technological by Indian Banks”	23.52%	N/A	India	[51]
“Internet Banking Cybersecurity Analysis in Developing Nations: User and bank perspectives: TAM & Statistical analysis”	52.2%	Supervised, unsupervised AI learning	Saudi Arabia, Pakistan, India	[52]
“Implementation of Hercules Architecture on Online Banking System”	N/A	Machine learning algorithm	China	[53]
“Cyber and Information environmental evaluation in the financial sector: Security Threats: Cyber Security Big data technology”	N/A	N/A	Malaysia	[54]
“Artificial Intelligence and its implementation throughout the Indian Banking System”	87%	ML, DL, NLG, NLP, Speed Recognition, Visual Recognition, Optical Character Recognition	India	[55]
“Information Security and its governance on Banking System”	86%	N/A	USA	[56]
“Artificial Intelligence impact on selected commercial Bank of India–Cost benefit analysis”	90%	ML, ANN, DL, NLP, CV, CC	India	[57]
“A Study of role emerging technology in current banking industry”	N/A	Artificial Intelligence, Cloud Computing, Machine Learning, IoT, Big data Analytics	India	[58]
“Technology Quality Management of the Industry 4.0 And Cybersecurity Risk Management on Current Banking Activities in Emerging Markets”	N/A	Technology for big data databases, cloud computing, machine learning, internet of things, artificial & business intelligence, data mining, and blockchain.	Vietnam	[59]
“Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges”	N/A	AI-powered malware.	Qatar	[60].

the manner in which they conduct affairs after discovering its potential. Following COVID-19, cyber dangers caused Indian’s Banks and India’s Reserve Bank to express grave concern. The serious issue is that many banks are currently at different phases of digital alteration, and ripeness degrees for vulnerability that determine bygone investment, scope contact clients, budget apportionment, and amenity stipulation. Regardless of the extent of cyber security in their institutions, bank managers must embrace new digitization and cyber security laws in order to meet business requirements and tackle COVID-19 issues. One of the biggest concerns facing the bank’s departments that analyze financial issues and fraud is how to use artificial intelligence technologies effectively in these areas [49]. As seen in Table III, suspicious activity, spam emails, and security weaknesses can all be tracked and predicted [50].

6.5. Research Gap in AI-Based CTI in Banking Sector Publications

This review paper explored different graphical and qualitative assessments of applications of artificial intelligence for cyber threat detection befalling the banking quarter revealed that research in this field started in 2003 with very few reports containing more conference papers. Although, studies did show that deep and machine learnings segment of artificial intelligence techniques have been used in Asia (India, Bangladesh, Qatar, Malaysia, China), North America (USA), and some parts of Europe (Vietnam) banking sector. The highest level of accuracy of the AI techniques used was obtained in Indian banks.

However, no study has shown that artificial intelligence has been applied to cyber threat detection in banks within Africa. Therefore, it can be deduced that AI has not been used to detect cyber threats in Nigeria or Africa. It could be due to the level of awareness and availability of technology or technical know-how. However, the issue of cyber threats has been reported in Nigeria and Africa at large by few researchers. Therefore, there is need for further studies on why AI has not been used to detect cyber threats in African or Nigerian banks since it has proven to be a very reliable method in cyber security.

7. Discussion

Data collection in lone scheme security vigilance and episode management using AI-based technologies has the potential to be a severe problem. Therefore, centralized data storage should be addressed by IT security rules. Data can be decentralized and disseminated. To solve this issue, decentralized blockchain technologies can be employed. Multiple servers should be used for data collection, along with numerous search heads. The difficulty faced by regulatory frameworks was another common subject. Most notably, a number of experts raised worry about laws that would prevent financial territory AI use. Due to the lack of legislative frameworks and ambiguity surrounding AI, these worries are understandable [45]. Some worries have been expressed about how AI technology can result in job losses, decreased customer loyalty, and data misuse [42]. As new regulation is created, it is therefore reasonable to assume that banks in Nigeria may confront additional difficulties in the future. All businesses are experiencing an increase in cyber-attacks, but the financial services sector is particularly vulnerable. Insurance, also banking industries are frequent beleaguered, according to the most recent statistics from security organizations [61]. Cyberspace-based threats having the power to disrupt large companies’

networks and access private information that might otherwise be protected by very sophisticated security measures. Throwing every bit of trust in cybersecurity experts may not be a highly effective way to stop cybercriminals from carrying out devastating assaults [62]. According to [60], financial institutions in Qatar have affected considerable stake favoring artificial intelligence and its potentialities in response to the need for more effective security systems.

AI, renowned attributable to its adaptability, offered incredible executive abilities depending on the available data. These gadgets have the ability to react intelligently based on the context and emotion of the scenario. Excellent encryption has been made possible by AI, and it is effective at detecting suspicious activity. Customers have used it to select loan amounts at enticing interest rates. Additionally, based on previous contacts, it has a greater grasp of clients and their behavior. These attributes elevate AI to the status of a hero for current and future generations. Traditionally, there seems to be a lot of anxiety about banking surety, AI however always improving to address indicated problems, creating a trustworthy foundation worldwide. Anyone can perform comprehensive encryption by equilibrating skill and appropriate usage. If applied appropriately, artificial intelligence potentially speeds up and renders anything more efficient. Artificial intelligence applications within banking have received lots of attention. However, a division from artificial intelligence called machine learning techniques is frequently employed in cyber security studies. Artificially powered Neural Network, Long Short-Term Memory Model and Supported Vector Machine have generally been shown to produce superior results than other methods. While Automata built with LSTM can effectively function with transient data, neural online-centralized replicas need more extensive data.

8. Conclusion

According to the publications, the Indian banking tract has prioritized cyber security according to predictive methods like machine learning and deep learning. Renowned and extensively applied AI method is machine learning. Reference [63] state that multiple implementations of AI challenges were investigated, given that security is regarded as among the greatest challenges. Unconventional AI methodologies are now being subjected to wide varied cyber-attacks aimed at compromising material or system privacy, authenticity, availability, and secrecy [64]. Although AI techniques are far more trustworthy and adaptable, they lead to improved security enforcement and superior protection against an increasing variety of advanced cyber threats. Artificial Intelligence and machine learning offer a powerful threat surveillance device to acquire a significant advantage over scammers and criminals [65].

References

[1] Definition: threat intelligence [Internet]. Gartner research. 2013. Available from: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence.

[2] Ramsdale A, Shiaeles S, Kolokotronis N. A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electron*. 2020;9(5):824.

[3] Brown S, Gommers J, Serrano O editors. From cyber security information sharing to threat management. *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, October 12, 2015, Denver Colorado USA New York, United States: Association for Computing Machinery.

[4] Liew A. Understanding data, information, knowledge and their inter-relationships. *J Knowl Manag Pract.* 2007;8(2):1–16.

[5] Dalziel H. How to define and build an effective cyber threat intelligence capability. Amsterdam, Netherlands: Syngress-Imprint of Elsevier; 2014. doi: 10.1016/B978-0-12-802730-1.00009-0

[6] Joint publication 2-0 joint intelligence [Internet]. Jt publication. 2013. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.

[7] Iancu N, Fortuna A, Barna C. *Countering Hybrid Threats: Lessons Learned from Ukraine*. Nieuwe Hemweg 6B, 1013 BG, Amesterdam, Netherlands: IOS Press; 2016.

[8] Definition of cyber-threat [Internet]. 2022. Available from: https://www.lexico.com/definition/cyberthreat.

[9] Oxford University Press. *Oxford Learner's Dictionaries*. Clarendon Street Oxford OX2 6DP: Oxford University Press; 2022.

[10] Malialis K. *Distributed Reinforcement Learning for Network Intrusion Response*. Heslington, York, Y010 5DD, England, United Kingdom: University of York; 2014.

[11] Kumar BS, Ch T, Raju RSP, Ratnakar M, Baba SD, Sudhakar N. Intrusion detection system-types and prevention. *Int J Comput Sci Inf Technol.* India. 2013;4(1):77–82.

[12] Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy. *IEEE Commun Lett.* 2013;18(1):114–7.

[13] Kacha CC, Shevade KA, Raghuwanshi KS. Improved snort intrusion detection system using modified pattern matching technique. *Int J Emerg Technol Adv Eng.* 2013;3(7):81–8.

[14] Jaiganesh V, Mangayarkarasi S, Sumathi P. Intrusion detection systems: a survey and analysis of classification techniques. *Int J Adv Res Comput Commun Eng.* 2013;2(4):1629–35.

[15] Bhattacharyya DK, Kalita JK. *DDoS: Attacks: Evolution, Detection, Prevention, Reaction and Tolerance*. Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742: CRC Press; 2016

[16] Jaber AN, Zolkipli MF, Shakir HA, Jassim MR. Host based intrusion detection and prevention model against DDoS attack in cloud computing. *Proceeding of the 12th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2017). International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. Barcelona, Spain: Springer; November 8–10, 2017.

[17] Rao VN, Suvarchala M. Customer perception towards banking services-post demonetization. *IOSR J Bus Manag (IOSR-JBM)*. 2018;20(4):79–86.

[18] Sujata D. A comparative study on pre and post demonetization on E-banking services. *IOSR J Bus Manag (IOSR-JBM)*. 2017;10(3):12–7.

[19] Alwan HA, Al-Zubi AI. Determinants of internet banking adoption among customers of commercial banks: an empirical study in the Jordanian banking sector. *Int J Bus Manag.* 2016;11(3):95–104.

[20] Kweyu M, Ngare P. Factor analysis of customers perception of mobile banking services in Kenya. *J Emerg Trends Econ Manag Sci*. 2014;5(1):1–8.

[21] Malik S, Noreen S, Awan AG. The impact of cybercrimes on the efficiency of banking sector of Pakistan. *Glob J Manag Soc Sci Humanit*. 2018;4(4):821–42.

[22] Ali L, Ali F, Surendran P, Thomas B. The effects of cyber threats on customer's behaviour in e-banking services. *Int J e-Educ e-Bus e-Manag e-Learn*. 2017;7(1):70–8.

[23] Lewis JA, Baker S. The economic impact of cybercrime and cyber espionage. Level 12, BA Building, John Street, Hawthorn, VIC 3122, Australia: Center for Strategic and International Studies; 2013.

[24] Njeru P, Gaitho V. Investigating extent to which cybercrime influences performance of commercial banks in Kenya. *Int J Econ Commerce Manag*. 2019;VII(8):489–514.

[25] Walden I. Computer crimes and digital investigations. *Int Comp Law Q*. 2007;57(4):997–998.

[26] Dalla EHaG MS. Cybercrime a threat to persons, property, government and societies. *Int J Adv Res Comp Sci Softw Eng*. 2013;3(5):997–1002.

[27] Hunton P. The growing phenomenon of crime and the internet: a cybercrime execution and analysis model. *Comput Law Secur Rev*. 2009;25(6):528–35.

[28] Ojeka SA, Egbide B-C. Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *Int Rev Manag Market*. 2017;7(2):340–6.

[29] PwC. Banking in Africa matters–African banking survey. 2016;1–100.

[30] Yayla AA, Hu Q. The effect of board of directors' IT awareness on CIO compensation and firm performance. *Decis Sci*. 2014;45(3):401–36.

[31] Asal V, Mauslein J, Young J, Cousins K, Bronk C. Repression, education, and politically motivated cyberattacks. *J Glob Secur Stud*. 2016;1(3):235–47. doi: 10.1093/jogss/ogw006.

[32] Gercke M. The slow wake ofAGlobal approach against cybercrime: the potential of the council of Europe convention on cybercrime as international model law. *Comput Law Rev Int*. 2006;7(5):140–5.

[33] Odunfa A. Nigeria: report on cyber threat calls for quick passage of 2012 bill. 2014. Online. http://www.allafrica.com/stories/201405080279.Html.

[34] McCorduck P. *Machines Who Think*. San Francisco, CalifETT79: WH Freeman and Company; 1979.

[35] Haenlein M, Kaplan A. A brief history of artificial intelligence: on the past, present, and future of artificial intelligence. *Calif Manag Rev*. 2019;61(4):5–14.

[36] Russell S, Norvig P. Artificial intelligence: a modern approach, global edition 4th. 2021;19:23.

[37] Russel S, Norvig P. Artificial intelligence—A modern approach. *Person Educ*. 2003, 736–41.

[38] Smith RG, Eckroth J. Building AI applications: yesterday, today, and tomorrow. *Ai Magaz*. 2017;38(1):6–22.

[39] Chui M, Manyika J, Miremadi M. *Where machines could replace humans-and where they can't (yet)*. *Online ed*. New York, 711 3rd Ave 4th Floor, United States: McKinsey & Company; 2016. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/.

[40] Truby J, Brown R, Dahdal A. Banking on AI: mandating a proactive approach to AI regulation in the financial sector. *Law Financ Markets Rev*. 2020;14(2):110–20.

[41] Caldwell M, Andrews JT, Tanay T, Griffin LD. AI-enabled future crime. *Crime Sci*. 2020;9(1):1–13.

[42] Kochhar K, Purohit H, Chutani R editors. The rise of artificial intelligence in banking sector. *The 5th International Conference on Educational Research and Practice (ICERP)*; 2019, Oct. 22–23, Palm Garden Hotel, Putrajaya, Malaysia.

[43] Shmuratko YA, Sheludko S. Financial technologies' impact on the development of banking. *Financ Credit Activity Probl Theor Pract*. 2019;4(31):61–9.

[44] Lukonga MI. Fintech, inclusive growth and cyber risks: focus on the MENAP and CCA regions. 2018.

[45] Mestikou MA, Smeti KE, Hachaichi Y. Artificial intelligence and machine learning in financial services market developments and financial stability implications. Available from: https://www.researchgate.net/profile/Yassine-Hachaichi/publication/369978046_Artificial_intelligence_and_machine_learning_in_financial_services_Market_developments_and_financial_stability_implications/links/6437d64e4e83cd0e2facd021/Artificial-intelligence-and-machine-learning-in-financial-services-Market-developments-and-financial-stability-implications.pdf.

[46] McNiff K. What is qualitative research. *The NVivo Blog: QSR Int*. 2016;9.

[47] Zamawe FC. The implication of using NVivo software in qualitative data analysis: evidence-based reflections. *Malawi Med J*. 2015;27(1):13–5.

[48] Soni N, Sharma EK, Singh N, Kapoor A. Impact of artificial intelligence on businesses: from research, innovation, market deployment to future shifts in business models. 2019. https://arxiv.org/ftp/arxiv/papers/1905/1905.02092.pdf.

[49] Kaur DN, Sahdev SL, Sharma DM, Siddiqui L. Banking 4.0: 'the influence of artificial intelligence on the banking industry & how ai is changing the face of modern day banks'. *Int J of Manag*. 2020:11(6). doi: 10.34218/IJM.11.6.2020.049.

[50] Meghani K. Use of artificial intelligence and blockchain in banking sector: a study of scheduled commercial banks in India. *Kishore Meghani Indian J Appl Res*. 2020;10(8). doi: 10.36106/ijar; ISSN No. 2249-555X.

[51] Sabharwal M. The use of artificial intelligence (AI) based technological applications by Indian banks. *Int J Artif Intell Agent Technol*. 2014;2(1):1–5.

[52] Alghazo JM, Kazmi Z, Latif G editors. Cyber security analysis of internet banking in emerging countries: user and bank perspectives. *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. November 1-December 2017, Salmabad, Bahrain: IEEE; 2017.

[53] Ou P, Wang H. Prediction of stock market index movement by ten data mining techniques. *Modern Appl Sci*. 2009;3(12):28–42.

[54] Jingxiong D. *Analysis of Cyber Security Threat Environment and Information Security System of Financial Industry Under New Situation*. Putra Nilai, Negri Sembilan, Malaysia: Manipal International University; 2020. https://www.researchgate.net/profile/Dang-Jingxiong/publication/338526977_Analysis_of_Cyber_Security_Threat_Environment_and_Information_Security_System_of_Financial_Industry_Under_New_Situation/links/5e196be7299bf10bc3a35355/Analysis-of-Cyber-Security-Threat-Environment-and-Information-Security-Systemof-Financial-Industry-Under-New-Situation.pdf.

[55] Parmar I, Agarwal N, Saxena S, Arora R, Gupta S, Dhiman H *et al.* Stock market prediction using machine learning. *2018 first International Conference on Secure cyber Computing and Communication (ICSCCC)*. October 11–13, 2018; Jalandhar, India: IEEE; 2018.

[56] Ula M, Ismail Z, Sidek ZM. A framework for the governance of information security in banking system. *J Inf Assur Cyber Secur*. 2011;1–12.

[57] Sindhu J, Namratha R. Impact of artificial intelligence in chosen Indian commercial bank-a cost benefit analysis. *Asian J Manag*. 2019;10(4):377–84.

[58] Kautikwar T. A study of role of emerging technology in current banking industry. 2020. http://dspace.vpmthane.org:8080/xmlui/.

[59] Nguyen TT, Nguyen ND, Vamplew P, Nahavandi S, Dazeley R, Lim CP. A multi-objective deep reinforcement learning framework. *Eng Appl Artif Intell*. 2020;96:103915. Available from: https://arxiv.org/ftp/arxiv/papers/1803/1803.02965.pdf.

[60] AL-Dosari K, Fetais N, Kucukvar M. Artificial intelligence and cyber defense system for banking industry: a qualitative study of AI applications and challenges. *Cybern syst*. 2022;1–29. doi: 10.1080/01969722.2022.2112539.

[61] Ryzhkova M, Soboleva E, Sazonova A, Chikov M editors. Consumers' perception of artificial intelligence in banking sector. *SHS Web of Conferences*. April 15–16, 2021; Yekaterinburg, Russia: EDP Sciences; 2021

[62] Perumal SV. Cyber security vital for Qatar's sustainable growth, say banks. *Gulf Times*. 2018.

[63] Petit J, Shladover SE. Potential cyberattacks on automated vehicles. *IEEE Trans Intell Transp Syst*. 2014;16(2):546–56.

[64] Cerrudo C, Apa L. Hacking robots before skynet. 2017;1–17. Available from: https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

[65] Dash P, Karimibiuki M, Pattabiraman K. Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques. *Digit Threats: Res Pract*. 2021;2(1):1–25. doi: 10.1145/3419474.