IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 June 2023, accepted 17 July 2023, date of publication 25 July 2023, date of current version 4 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3298824

RESEARCH ARTICLE

Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis

HABIB ULLAH KHAN[1], MUHAMMAD ZAIN MALIK[1], SHAH NAZIR[2], (Member, IEEE), AND FAHEEM KHAN[3]

[1]Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar
[2]Department of Computer Science, University of Swabi, Swabi 23430, Pakistan
[3]Department of Computer Engineering, Gachon University, Seongnam-si 13120, South Korea

Corresponding authors: Habib Ullah Khan (habib.khan@qu.edu.qa) and Faheem Khan (faheem@gachon.ac.kr)

This work was supported in part by the Qatar National Library, Doha, Qatar; and in part by the Qatar University Internal Grant under Grant IRCC-2021-010.

ABSTRACT Biometric authentication is gaining the interest of private, public, consumer electronics and corporate security systems. For the protection of cyberspace from hackers and other harmful people, biometric security is growing more and more popular among organizations, individuals and enterprises. The word ''cyber security'' refers to the procedures, techniques, and tools used to safeguard data, network system, computer networks and software from potential attacks online. Online financial service delivery is referred to as ''cyber banking.'' As the trend of exchanging things has changed, internet banking has grown. Despite the benefits, there have been instances of security threat-related issues with Internet banking. To identify persons, biometric security verifies their physical attributes and behavioral traits. For identification verification, it is the most reliable and effective physical security method. According to biometric authentication, people can be recognized precisely based on their innate behavioral or physical traits. Numerous security measures have been implemented throughout the entire Internet banking service to address these issues. Globally, cybercrime has deep roots and poses a significant threat to the occurrence of criminal or terrorist behavior. Without being addressed by a single authority, these risks can compromise security on the inside as well as the outside. If the cybercrime goes unnoticed, both money and personal data are lost. Internet services and information infrastructure have previously been targeted in assaults. Online fraud and hacker attacks are only two examples of the daily computer-related crimes that take place. The Internet of Things (IoT) is the most reliable foundation for facilitating high-quality, comfortable human living. IoT has had a substantial impact across a range of application domains. Smart gadgets are more vulnerable to hackers because of their rapid development and trust in wireless mechanics for data transport. As a result, the rate of cybercrime is rising daily. Artificial Intelligence (AI)-based cybersecurity emerges because of technological advancement and poses a risk to public safety, personal property rights, and privacy protection for people. The study elaborates on the key features of biometrics system in conventional and Islamic banking to counter the risk of cybersecurity and provide high safety and security to the banking industry. For this systematic literature review, the most suitable and most relevant 101 articles from the reputed online libraries are selected. This analysis absorbed four research questions and pertinent keywords from the period of 2009 to 2022 (a part of 2023 was included).

INDEX TERMS Biometrics, cybersecurity, cybercrime, systematic literature review, FinTech, conventional & Islamic banking, financial security.

The associate editor coordinating the review of this manuscript and approving it for publication was Vincenzo Conti.

I. INTRODUCTION

Cybercrime is a more specialized definition of illegal behavior centered on the internet and IT. Attacks by cybercriminals

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

pose a progressively more difficult problem, particularly for developing nations. The goal of international cyber terrorism is to acquire sensitive information so that it can be used to gain complete control and substantial advantages. In recent years, banking industry has been hit by a global economic crisis that has forced it to restructure, particularly in some nations. Furthermore, both individual and industrial consumers have lost faith in the banking system, which has been severely harmed. In today's harsh business environment, banks are finding it particularly difficult to recruit new clients [1]. The unique physical features like fingerprints, finger scanning and facial Geometry which help to recognize the individual is known as biometric. This technology is mostly employed for identification, access control and the identification of those who are being watched. Biometrics are mostly used by security systems in settings where physical security is important, and theft is a worry. During the worldwide financial crisis, banks were under a lot of pressure to keep their liquidity levels up. In general, empirical data demonstrates that banks with adequate liquidity can satisfy their payment commitments, but banks with insufficient liquidity are unable to do so. With funding sources dwindling and worries about asset value and capital adequacy surfacing, the GFC demonstrated how fast liquidity risk can spread [2]. Since most finance and banking services and information are now located on the cloud, critical financial data should be protected by an artificial intelligent-based scalable and flexible access control system. Financial organizations can utilize systems that include encryption, two-factor authentication, and authorization as built-in security features. However, access controls are more important than infrastructure and property in protecting consumers and company information. Banks that decide to increase their noninterest revenue operations are faced with fiercer interbank competition as a result of the major financial liberalization and globalization expansion in order to expand, achieve efficiency, and lower idiosyncratic risk [3], [4].

Financial terrorism is shown by the current worry over cyber security on a worldwide scale. The most difficult problem in the context of modern internet banking has been securing customer data. In the financial sector, cyberattacks are getting more and more serious. Artificial intelligence is being used by the banking sector to build cyber defense systems to reduce unwanted access and cyberattacks. Banks in Qatar are aware of the danger posed by cybercrime and the importance of cybersecurity for long-term development. The banking sector is now going through a significant technological change. Understanding how emerging technologies like artificial intelligence (AI) affect banks' cybersecurity becomes crucial [5]. The development of FinTech and other technologies like IoT, Big Data, blockchain, artificial intelligence (AI), and machine learning are occurring simultaneously in the banking and financial services industry [6]. The recent financial crisis has highlighted the significance of preserving financial stability and highlighted the complexity and nonlinearity of the banking systemic risk phenomena. Recent financial crises have demonstrated that banking crises are frequently at the center of larger financial crises. As a result, maintaining financial stability depends on the health of the banking industry. The transfer of economic resources, liquidation and payment, financing and equity refining, risk management, information providing, and incentive provision are only a few of the fundamental duties performed by financial systems [7], [8]. The banking system is an essential component of contemporary finance and a critical area of study for ensuring the smooth operation of the financial system. Banks establish intricate ties via interbank market in the forms of loan, payment, discount, settlement, guarantee, acceptance, and so forth [9].

Cybersecurity and cybercrime are interrelated. Security managers must maintain a secure company environment by strengthening security layers and safeguarding information infrastructure. Computers are either used as the target of the crime or as a storage medium for cybercrimes. Computers may act as both a target and a storage device, depending on how the information they hold is changed or accessed. Computers can store data that will help in the commission of a crime. ICT has had unforeseen repercussions that have increased awareness of many cybercrimes. Different industries have been impacted by cybercrime, and the banking industry is one of them. This sector has seen various cybercrimes, such as ATM frauds, Phishing, identity theft, and denial of service attacks [10], [11]. A combination of biometrics is also used by certain banks. This implies that when multi-factor authentication and biometrics verification are used together, an almost impenetrable layer of security is produced. Many banking sectors use data mining tools for customer segmentation and productivity, advertising, credit ratings and authorization, payment default, and frauds transactions, among other things. More than ever, there is a risk of cybercrime. Cyber fraud and criminal activity carried out via use of electronic equipment like mobile phones, computers and other network devices fall under a category of crimes that are transitional in nature compared to traditional crimes. In accordance with their skill set, ambitions, and objectives, cybercriminals employ a variety of techniques. The biggest issue for financial institutions in the twenty-first century is the exponential increase of cybercrimes, and protecting the internet is now more important than ever [12], [13], [14]. The benefit of this research to help the various bank and financial organizations and regulatory department to counter the risk of cybercrime. This research highlights the below point:

- To determine the primary issues facing in the banking and finance industry, to locate potential solutions, to suggest new direction for ongoing study in the suggested area, and to fill gap and in the available solutions that may have emerged.
- To enhance the competences of existing system to secure the banking and financial sectors by using the new approach to provide high protection in the organizations.

- To highlight the biometrics system across a variety of areas to examine the impact of biometrics that can affects banking to prevent cybercrime.
- To explain the key feature of biometrics system which can help the banking sector to prevent cybercrime.

II. LITERATURE REVIEW

One of the fastest expanding areas of the global financial markets is Islamic finance and capital markets. The financial industry's environment has transformed as a result of recent advancements in Islamic finance and the capital market. Islamic banking has seen explosive expansion and is now a viable option for investors and depositors throughout the world. Despite the mismatch between the current financial structure and business practices, Islamic banking is expanding at a rate that hasn't been seen in the past 20 years. With operations in more than 50 countries, the amount of Islamic banking reached US$951 billion at the end of 2008. Although Islamic banking is facing many challenges, three of them are crucial to the industry's survival, the first is Sharia compliance in its operations in a setting where interest-based practices are prevalent, especially in Muslim cultures [15], [16], [17], [18]. The second factor is how professionals in the financial sector see the system's performance and its capacity to meet all of trade and industry's demands. Third is how many Muslims see whether current Islamic banking activities are Sharia compatible or simply copies of Western processes cloaked under the Sharia name. FinTech is the combination of finance and technology. According to the laws and guidelines outlined by Shariah, Islamic finance offers its clients financial services. FinTech has grown rapidly over the past ten years, just like Islamic finance has over the past two decades. Islamic finance's major goal is to employ Shariah-compliant financial instruments to accelerate social and economic development. Financial stability board define the FinTech as ''FinTech is technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services'' [19], [20], [21], [22], [23].

Online banking is referred to as ''cyber banking,'' whereas the term ''cyber security'' refers to the techniques, tools, and policies developed to resist cyberattacks. Cybersecurity threats, a form of financial terrorism, are currently affecting everyone in the globe. The safeguarding of user privacy has proven to be the most difficult part of contemporary internet banking. The convenience of banking operations has been greatly enhanced by technological advancements, but at the same time, a variety of new types of cybersecurity issues are emerging and reaching a peak. A person is recognized by a face recognition system using their facial architecture. It may be utilized in a variety of contexts, such as credit card transactions, law enforcement and mobile devices. Even though there are several procedures currently in place to counteract these crimes, there are still numerous weaknesses in all information systems. Financial institutions must create prediction models that can be applied to the fight against cybercrime. To detect malicious activity, systems require ongoing, efficient monitoring, operation, and tracking of transactions. This is only possible by utilizing cyber-resilient technology to ensure information security [24]. Insider threats of growing cyberattacks are frequently exposed to data breaches when cybercrime is generating significant economic damage. To reconstruct a crime, law enforcement authorities (LEAs) must provide enough evidence, make specific observations and interpretations of the digital data, and demonstrate the suspect's unauthorized use of the computer. Continuous monitoring is strongly advised as a component of information security measures in insider risk management when complete network activity protection is required to safeguard sensitive and personal data [25], [26], [27].

Absolute cybersecurity cannot be guaranteed, not even with biometric technologies. Although breaches are much less likely with biometric security than with password security, they are still possible. Even though biometric cybersecurity uses high-quality cameras and other sensors, attackers can still target them. Internet protection against cyberattacks is achieved by the usage of cybersecurity. Because breaches can harm a company's reputation as well as its clients financially and non-financially, cybersecurity is meant to prevent them. In the recent years, artificial intelligence, big data, 5G and other technologies have recently permeated and been implemented in a variety of areas. Major bank outlets are seeking a fusion of cutting-edge technology and financial services. Applications of artificial intelligence may be found in a wide range of fields including manufacturing, finance, education, communication, business, government, service and more. Our daily lives are being progressively impacted by artificial intelligence. The world's growth and progress will be greatly influenced by how it uses data and connected technologies. AI has the power to significantly change our lives either for the better or worse. Criminal identification is also being aided by biometrics. It is being investigated in a variety of ways as a resource for public safety [26]. Biometric payment method is one of the uses of biometrics in finance. Fingerprint scans are frequently utilized in conjunction with this technology to authorize transaction operations.

III. RESEARCH METHODOLOGY

A systematic literature review was carried out to thoroughly analyze the various cyber-attacks in the domain of banking sector. Systemic literature review (SLR) is described as ''a method of identifying, interpreting and evaluating all existing research related to a specific topic area, phenomenon of interest or research questions (RQs). The main objectives of an SLR, as opposed to a spontaneous or ''at-will'' limiting the study's scope and ensuring that enough high-quality papers are retrieved are the goals of the literature review. The SLR technique aims to avoid evaluating findings only partially. Biasness in primary research activity, however, cannot be eliminated. Phases of SLR include planning, conducting,

and reviewing. To eliminate researcher prejudice and organize the confusing data, a review paradigm is developed as part of the planning process. This paradigm directs all subsequent phases. Different search difficulties are described by the approach. The search strategy specifies sources and the time frame for which the future research will be conducted, justifications for choosing sources, search criteria and other restrictions, quality assurance criteria that specify the procedure for data extraction and retrieval should be followed whether the research is to be included or excluded, as well as procedures for storing search files and data extraction. By working together, the writers implement the suggested SLR. Based on the writers' opinions, several studies were examined, analyzed, and assessed. Studies that don't support the assessment criteria are omitted from consideration after being sorted out and analyzed according to particular criteria. Using the concept from a review paradigm was put into practice. The review paradigm entails a summary of the research question(s), the topic selection, a search strategy, the examination and obtaining articles, the evaluation of the articles' quality, and data synthesis.

A. SELECTING RESEARCH DOMAIN

To have a better understanding of cybersecurity concerns, a thorough investigation of the security topic was carried out. To comprehend the concept of cybersecurity, identify problems in the field, and discover what professionals have done thus far to address the challenges, research papers from a variety of digital information sources were thoroughly analyzed.

B. RESEARCH QUESTIONS FORMULATION

The objectives of this study are fourfold: to identify the key biometrics that affect banking to prevent cybercrime; to highlight how biometrics system and FinTech has an influence on the financial sector. To enhance the capabilities of the present system to protect the financial sector, it is necessary to study the primary benefits experienced by the banking industry while using biometrics systems. Research was done on pertinent papers, conference proceedings, book chapters, journals, and book chapters that specifically described security problems. Our first findings indicated that cyber security is a significant endeavor. To make this review briefer, it was recommended that the research be conducted with a specific focus on addressing the research questions listed in "Formulation of Research questions (RQs)" table 1 which were developed after the examination of various publications and articles.

C. STRINGS BASED SEARCHING

The search approach is made up of searching the keywords and search methodology. The descriptions are provided in a sequence of actions. The procedures below are completed for keyword creation. Major important phrases were found in the suggested research topics. The major words' synonyms were filtered out for efficiency.

TABLE 1. Formulation of research questions.

S.No	RQs	Explanation
Q1.	What are the key features of biometrics system that affect banking and prevent cyberattacks?	The purpose of this question is to describe the various features that can affect banking to prevent cybersecurity by utilising the biometrics system.
Q2.	How does cybercrime influence FinTech in the banking sector?	FinTech is an emerging technology that can influence the banking sector. The aim of the research question is to secure the transaction between the parties by using financial technology and its features.
Q3.	What are the key benefits gained by the banking sector using biometric systems after overcoming cyberattacks?	As the banking sector shifts its business from a traditional to a modern global environment, the risk of cyberattacks and cybercrime is increasing day by day. The aim of this RQ is to provide smooth and secure operations by using biometrics technology to overcome the risk of cyberattack.
Q4.	Using the literature as evidence, how can we enhance the competence of the existing system to secure the banking sector?	By overcoming cyberattacks, what are the major benefits brought to financial organisations? This RQ aims to enhance the competencies of existing available systems to secure the banking sector, enhance customer satisfaction and trustworthiness levels, and build a bridge between banks and clients.

- For the development of Keyword, books and articles were examined.
- Boolean OR was used to align the synonyms.
- For connecting Main words, Boolean AND is employed.

A generic query is created by concatenating the terms. ("biometrics" OR "fingerprint" OR "face recognition" AND "cybercrime" OR "criminology" OR "fraud" AND "cybersecurity" or " cyberattack" AND "banking" OR "banks" OR "financial organizations" OR "banking sectors" AND) is formed.

D. THE SEARCHING PROCESSES

To gather information from many researchers' works in cybersecurity for synchronization, the second author of this article did a comprehensive and thorough review of the recommended study on 4digital libraries. The following digital libraries were searched for relevant research articles: IEEE Xplore, Science Direct, Hindawi, and Taylor & Francis. The complete reviewing procedure is shown in Figure 1. The planned research was completed by looking at the titles, abstracts, and index terms of previously published research publications, including journal articles, conference papers, and book chapters. To avoid article duplication, articles are downloaded and looked up from pertinent libraries. There are several stages to the search process in this study.

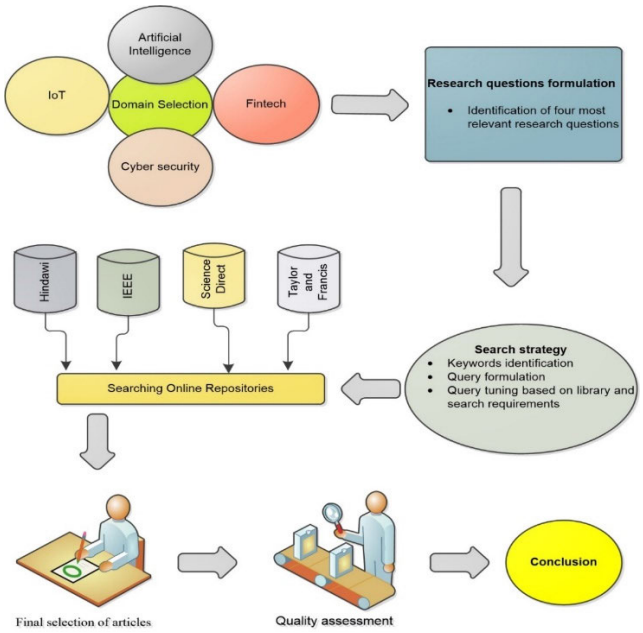


FIGURE 1. Process adopted for SLR.

TABLE 2. Detail of selected articles.

	IEEE Xplore	Science Direct	Hindawi	Taylor & Francis
Conferences	334	44	8	-
Journals	19	333	316	286
Books	21	11	-	15
Magazines	8	-	-	-
Books Chapters	-	97	-	-
Case report	-	-	93	-
case series	-	-	13	-
Editorial	-	-	71	4
Others	-	-	44	19

Phase 1 – To find publications relevant to the proposed topic, four digital libraries are systematically examined. The search's findings were categorized as perspective studies.

Phase 2 - Articles are obtained from these libraries on the bases of keyword string.

Phase 3 – Relevant studies are mined from the online digital libraries.

The most four peer reviewed online repositories have chosen for this SLR process. The percentage contribution of each online library is shown in Figure 9 work including IEEE explore, Hindawi, ScienceDirect and Taylor and Francis. IEEE and ScienceDirect have contributed the most in the research domain.

After using the Table 2 to analyze them it represents of selected articles inclusion and exclusion standards. Figure 2 shows the overall quantity of papers selected on the bases of keywords and string. A set of total number of articles each year is shown in Figure 3. It also shows that after 2018, the volume of paper steadily grows, which illustrates how biometric technology has been applied and used in the financial and banking industries. The distribution of articles by year for the different libraries is shown in Figure 3 (2009–2022) a part of 2023 included.

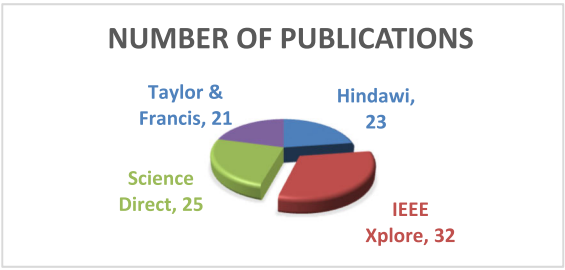


FIGURE 2. Digital repositories libraries for SLR work.

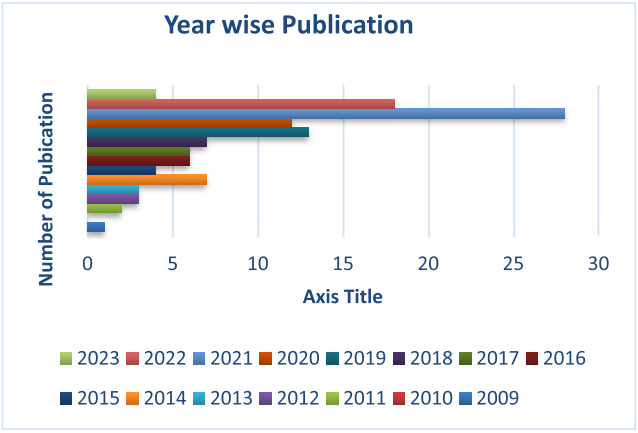


FIGURE 3. Trend of AI in the proposed domain from 2009 to 2022 (A part of 2023 included).

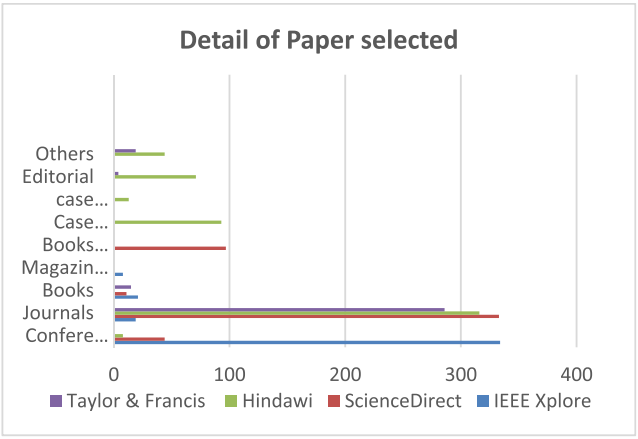


FIGURE 4. Paper details selected for SLR.

TABLE 3. Selection of primary research.

Online databases	Filter by keywords based	Filtered by title	Filter by abstract	Filter by contents
Hindawi	7659	279	98	23
IEEE Xplore	11715	301	114	32
Science Direct	13472	332	125	25
Taylor	9761	371	132	21
Total	42607	1283	469	101

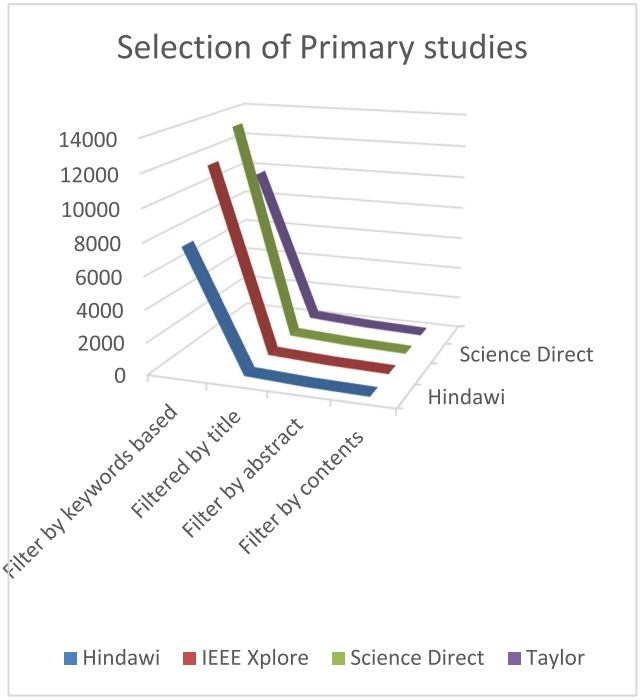


FIGURE 5. Detail of selection paper.

The selection criteria of paper (journal papers, case reports, conference papers, book chapters, magazines, and survey papers) are shown in Figure 4.

E. SCRUTINIZATION AND RETRIEVAL OF RELEVANT ARTICLES

Four digital databases were examined as part of the search procedure, yielding 1283 research papers. The proportion of studies found is shown in Figure 5 and table 3 represents the number of studies found. Metadata was found in the initial search phase (keyword, title, abstract and the contents). To locate relevant journal papers for study as the initial search turned up 1283 randomized studies, scrutiny (Table 3) was necessary. One of the authors of this paper (3rd author), carefully examined and checked the titles of pertinent studies after gathering meta data. This will help to minimize the number of articles, meaning that those that are pertinent to our research area are skipped over and appropriate ones are taken into consideration for further analysis. This process is required to remove irrelevant and duplicate study title-based paper selections from the 101 articles shown in Table 3 and Figure 5.

F. QUALITY OF ASSESSMENT AND DATA SYNTHESIS

Quality evaluation criteria were applied based on the filtered studies found after carefully examining and retrieving pertinent publications, i.e., each article was carefully reviewed to see if the research addressed at least two specified questions. The three writers of this study each made an equal contribution throughout this stage. To answer the questions,

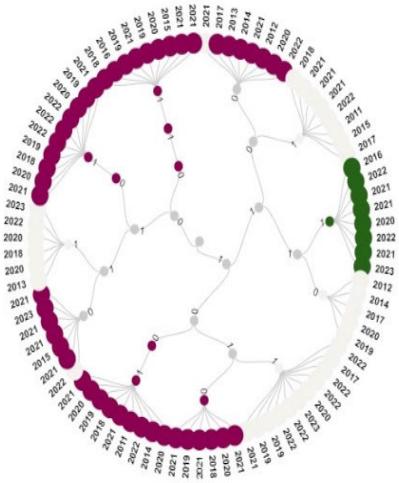


FIGURE 6. Quality assessments.

this phase aims to compile and analyze the data. A manual scoring method was utilized to carefully pick and check the data that was found to evaluate the relevant study. It was confirmed whether these studies could respond to research topics. Such concerns are covered in Figure 6 and Table 4. (i.e., answering at least 2 RQs). There are just two options for each question. Specifically, ''yes'' is equal to 1 and ''no'' is equal to 0. The overall response to the questions posed is used to calculate the reliability value for each research. By evaluating pertinent papers with a focus on responding to two or four research questions, the validity of the proposed study was established. In accordance with the paper score, 61 papers were discarded after the QoA test was applied to content-based articles and abstract that were retrieved, around 101 published research work that could answer minimum two predetermined research questions. Figure 6 and Table 4 lists the ratings for the quality of the articles that were chosen. The RQ1 extracts a detailed explanation of the key characteristics of biometrics that can affects banking and financial sector to prevent the cybersecurity entities from a few chosen studies, while the RQ2 explain the influence of FinTech in the banking and financial industry. RQ3 is concerned with key benefits gained by the banking sector using biometrics system after overcoming the cybercrime. RQ4 provides how we can enhance the competences of existing system to secure the banking sector from the risk of cyberattack. Table 4 shows the results of the assessment of pertinent publications using the evaluation criteria.

IV. RESULTS AND DISCUSSIONS

A Each research question is explored in the following subsections, which also categorize the pertinent publications according to the research questions posed. Based on the research question, a summary of each research article is given as below.

TABLE 4. Quality assessment scoring table for most suitable articles.

Q1	Q2	Q3	Q4	Score	Reference	Year
1	1	1	1	4	[1]	2016
1	1	1	0	3	[2]	2012
0	1	1	0	3	[3]	2022
1	1	1	1	4	[4]	2022
1	1	1	0	3	[34]	2014
1	1	0	0	3	[8]	2021
1	1	1	1	4	[29]	2021
1	1	1	1	4	[43]	2021
1	1	1	1	4	[44]	2020
1	1	1	1	4	[80]	2022
0	1	0	1	2	[81]	2021
1	1	0	0	2	[46]	2017
1	1	0	0	2	[7]	2013
0	1		1	2	[77]	2020
1	0	1	1	3	[47]	2022
1	1	0	1	3	[32]	2018
1	0	1	1	3	[52]	2017
0	1	1	1	3	[97]	2013
1	1	0	1	3	[9]	2021
1	1	0	1	3	[54]	2021
1	1	0	0	2	[21]	2014
0	1	1	0	2	[56]	2021
0	0	1	1	2	[58]	2018
0	1	1	0	2	[59]	2015
1	0	1	0	2	[57]	2021
1	1	0	1	3	[24]	2021
0	1	0	1	2	[100]	2018
0	1	0	1	2	[25]	2019
1	1	1	0	3	[19]	2017
1	0	1	0	2	[23]	2020
1	1	0	1	3	[5]	2022
1	1	0	0	2	[16]	2021
1	1	0	1	3	[91]	2011
1	1	1	0	3	[60]	2020
1	1	0	1	3	[61]	2015
1	1	0	0	2	[98]	2012
0	1	1	0	2	[78]	2021
1	0	0	1	2	[6]	2020
1	0	0	1	2	[17]	2014
1	1	1	0	3	[15]	2019
1	1	1	1	4	[63]	2021
0	1	0	1	2	[94]	2022
0	1	0	1	2	[92]	2022
1	0	0	1	2	[45]	2022
0	1	0	1	2	[82]	2022
1	1	0	0	2	[33]	2020
0	1	1	1	3	[83]	2020
1	1	0	0	2	[64]	2022
1	0	1	0	2	[65]	2018
0	0	1	1	2	[84]	2016
0	1	1	0	2	[74]	2021
0	1	1	1	3	[76]	2018
0	1	0	1	2	[71]	2020
0	1	1	1	3	[72]	2020
0	1	0	1	2	[55]	2019
0	0	1	1	2	[85]	2019
0	1	1	1	3	[75]	2022
1	0	1	0	2	[66]	2021
1	0	1	0	2	[67]	2019

TABLE 4. *(Continued.)* **Quality assessment scoring table for most suitable articles.**

0	0	1	1	2	[86]	2021
1	0	1	1	3	[68]	2022
1	0	0	1	2	[30]	2011
0	0	1	1	2	[89]	2019
1	0	1	1	3	[62]	2022
0	0	1	1	2	[90]	2020
1	0	1	0	2	[35]	2021
0	0	1	1	2	[87]	2015
0	1	0	1	2	[79]	2021
1	1	0	1	3	[101]	2017
1	1	1	1	4	[53]	2023
0	1	1	1	3	[96]	2023
1	0	1	1	3	[36]	2020
1	0	1	1	3	[93]	2023
1	0	1	1	3	[37]	2022
1	0	1	1	3	[38]	2022
0	0	1	1	2	[95]	2021
1	0	0	1	2	[42]	2021
0	0	1	1	2	[88]	2021
1	0	0	1	2	[69]	2018
1	0	1	1	3	[48]	2019
1	0	1	1	3	[50]	2019
1	0	0	1	2	[39]	2019
1	0	0	1	2	[49]	2020
1	0	1	1	3	[51]	2021
1	0	0	1	2	[40]	2021
0	1	1	0	2	[73]	2023
0	1	1	0	2	[70]	2021

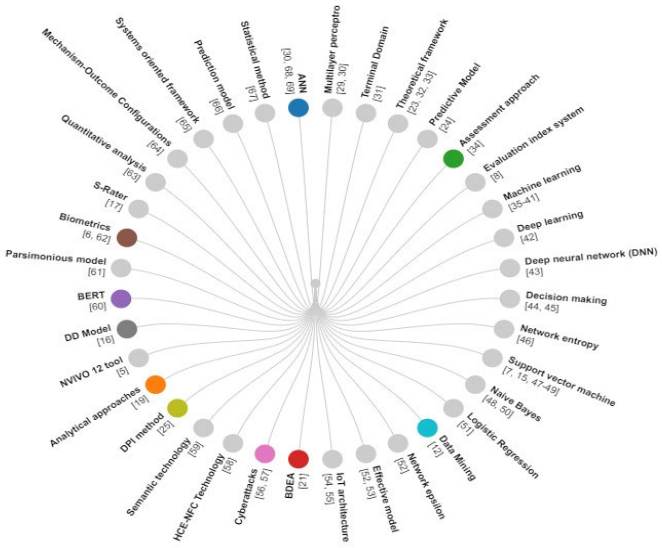


FIGURE 7. Feature of AI prevent cybercrime.

RQ 1. What are the key features of biometrics system that affect banking and prevent cyberattacks?

Today, every country in the globe is dealing with some sort of crime, and the growing population has made the problem even worse. Cybercrime attacks pose a substantial danger in a globalized economy, and for this reason alone, they shouldn't be disregarded. The increased spread of cybercrimes in developing countries is a current trend [28]. Figure 7 and Table 5 show the different feature of AI that can affects banking sector to prevent the risk of cybercrime.

RQ 2. How does cybercrime influence FinTech in the banking sector?

FinTech is now among the industries that create new business and job in the financial market. It is become the

TABLE 5. List of key features to prevent cybercrime.

	Feature to prevent cybercrime	Description	References
1.	Multilayer perceptron neural network	The study investigates the primary impact of electronic banking on the structure of the Iranian banking sector. By using the MPNN and fuzzy regression to electronic banking	[29, 30]
2.	Terminal Domain	The major elements of this study to present the security methods used in the domain of terminal user. Authors categorize the security-based system in the domain of terminal user into the following categories: secure keyboard programs, personal firewalls, E2E encryption, PKI applications, antihacking programs, ant reverse engineering method and remove media security we describe in-depth and key method of every security system.	[31]
3.	Theoretical framework	The authors offer a theoretical framework to analyse the systemic risk of the banking system by examining the temporal evolution of the risk across time using sequences of financial data.	[23, 32, 33]
4.	Predictive Model	The article explains how to create predictive models that may be applied to stop cybercrime in the financial institutes.	[24]
5.	Assessment approach	To identify domestic systemically significant banks (D-SIBs) in China, the Basel Committee recommended the official assessment approach, to which this article responds.	[34]
6.	Evaluation index system	This article investigates the assessment of the real economy as provided by fintech based on fintech advancement to close the gap. First, a data envelopment analysis evaluation index method was created to gauge the effectiveness of fintech services	[8]
7.	Machine learning	This study uses machine learning methods to pinpoint the major forces influencing financial growth in Africa.	[35-41]
8.	Deep learning	In the financial industry, deep learning and machine learning techniques are commonly used to assist payments, mobile banking, trading, and client credit decisions.	[42]
9.	Deep neural network (DNN)	In this study, authors provide an integrated AI-based approach that combines the random frog algorithm (RF), the generalized additive model (GA), and the DNN to forecast the Fintech index.	[43]
10.	Decision making	The authors also include fintech saturation as an inception variable for the model and discover that if fintech penetration is higher than the threshold, financial literacy has a bigger influence on decision making in financial technology.	[44, 45]
11.	Network entropy	The researcher examines the network entropy in the banking system in interbank network and analyzed the random networks with world networks and free scale networks	[46]
12.	Support vector machine	In these studies, authors use SVM to forecast a systemic risk in banking an effort to propose a novel model with improved stability and explanatory power.	[7, 15, 47-49]
13.	Naive Bayes	In this paper the execution of Support Vector Machine Naive Bayes, Logistic Regression and K-Nearest Neighbor on highly distorted data fraud in credit card is examined.	[48, 50]
14.	Logistic Regression	This study uses a variety of machine learning and deep learning techniques to identify credit card fraud. Various algorithms, including Logistic Regression Naive Bayes, KNN, Sequential Convolutional Neural Network and Random Forest are skewed to train the network on both normal and abnormal transaction features.	[51]
15.	Data Mining	In order to investigate the cybercrime data sets and organize the solvable issues, this work employs unique data mining methods as Influenced Association Classifier, K-Means and J48 Prediction tree.	[12]
16.	Network epsilon	The objective of this study is to assess the performance of the banking sector by using a network epsilon-based measure model that integrates radial and non-radial measures of efficiency into the network production process framework with NPLs.	[52]
17.	Effective model	Based on an analysis of the influence of Fintech on corporate technological innovation using a panel fixed effects model, this research investigates the potential impact mechanism of Fintech on enterprise technological innovation.	[52, 53]
18.	IoT architecture	An overview of the IoT framework, which includes IoT architecture, technologies, and protocols, is provided in this review article. Each layer's specific security concerns are covered in detail, as well as any necessary countermeasures.	[54, 55]
19.	BDEA	The effectiveness of twelve Islamic banks in Malaysia was examined using the Bootstrapping Data Envelopment Analysis (BDEA) methodology.	[21]

TABLE 5. *(Continued.)* **List of key features to prevent cybercrime.**

20.	Cyberattacks	This study suggests strategies that might assist experts and analysts in utilizing untapped Fintech potential and suggests corrective actions for reducing cyberattacks.	[56, 57]
21.	HCE-NFC Technology	Using HCE-NFC Technology, a series of security guidelines for e-wallet apps presented in the paper to minimize the risk factor.	[58]
22.	Semantic technology	This research explores how semantic technology may improve the effectiveness of cybercrime investigation.	[59]
23.	DPI method	This article introduces the DPI method, which may assist investigators in creating fresh approaches and carrying out the digital investigative process in a timely and forensically sound manner.	[25]
24.	Analytical approaches	By using computational and analytical methods to mine the Qur'an and the Hadith for hidden information about Islamic financial business operations, this study aims to build and develop business procedures.	[19]
25.	NVIVO 12 tool	Using the NVIVO 12 tool, a qualitative thematic analysis of bank cyber security was carried out.	[5]
26.	DD Model	The proposed IFSB regulation's impact on the performance of Islamic bank stocks is assessed using the difference-in-differences model (DD) in this research.	[16]
27.	BERT	Researchers select 25,580 FinTech patent applications that were filed to the US and European Patent Offices between 2000 and 2017 using our best BERT-based model on a huge dataset of financial patent abstracts.	[60]
28.	Parsimonious model	The purpose of this study is to discover characteristics that influence Internet users' desire to utilize online services. It does this by presenting a sparse model that draws on criminological ideas and studies on technological adoption.	[61]
29.	Biometrics	The paper suggests biometric online banking system aims to help reduce the amount of cybercrime that occurs when people use online banking and tends to increase the user trust in doing so.	[6, 62]
30.	S-Rater	The paper aim to implement the S-Rating model using data mining approach in the web application.	[17]
31.	Quantitative analysis	To thoroughly understand the FinTech challenges that are now having an impact on the caliber of FinTech mobile apps, a quantitative analysis was applied to the data that was gathered.	[63]
32.	Mechanism-Outcome Configurations	To build the refine programmed theory and create Mechanism-Outcome Configurations (CMOCs) which explain why, how and under the circumstances old adults become victims of financial cybercrime, based on the 52 primary and secondary data collection researchers then extrapolated this information to consider logical intervention strategies.	[64]
33.	Systems oriented framework	The paper provides a conceptual paradigm for tracking money laundering that is systems-oriented by setting out a plan for enhancing money laundering detection.	[65]
34.	Prediction model	The research proposed a revised prediction model for customer loyalty in Islamic finance has been developed.	[66]
35.	Statistical method	This study explains the statistical method that demonstrated a substantial positive correlation between sustainability practices and the performance of financial metrics in Islamic banks from the management and shareholder perspectives.	[67]
36.	ANN	The goal of this study is to develop an artificial neural network model machine learning to assess the probability of money laundering in banks.	[30, 68, 69]

second largest industry of FinTech in the world. FinTech has received a lot of attention recently because of its rapid advancement. FinTech's growth has been hailed by many observers who believe that it can drastically change financial services by making transactions more affordable, convenient, and secure. A consistent definition of the current idea of FinTech has not yet been established. However, the word ''FinTech'' first appeared in a related Citibank paper in 1993. Due to the profound changes it has wrought in financial services, FinTech has received a lot of attention in the world of financial industry has been referred to as the ''FinTech revolution'' by some analysts [15], [53], [60]. Regulators and decision-makers are figuring out the best solutions to overcome data gaps brought on by the FinTech industry. These gaps have often been caused by actions taken by FinTech companies that operate outside of the regulatory framework and are not required to provide information about their operations [70]. It has being used and abused by criminals for money laundering, extortion, deception and funding of illegal activity [71], [72], [73]. Aside from this positive aspect, FinTech adoption takes time, costs a lot to maintain, upgrade, and educate both customers and workers, and there is a risk of failure [74], [75]. The slow emergence of attempts to integrate technology and finance has been accelerated by the ongoing improvement of Internet financial practices and the change of the financial industry [76].

TABLE 6. List of key benefits gained by banking sector after minimize the cybercrime.

S.No	Key Benefits	Description	References
1.	Increase in share	The implemented study of the causes of this decline demonstrates that the decline in the percentage of banks is attributable to a rise in the share of small banks.	[29]
2.	Prediction accuracy	These findings show that the suggested RF-GA-DNN prediction method considerably shortens convergence time while promising high prediction accuracy.	[43]
3.	Stability	According to our interpretation, investors view the new legislation for Islamic banks as an indication that their financial soundness has increased, far outpacing the expenses associated with increasing capital requirements.	[16]
4.	Positive effects	The findings demonstrate that involvement in the financial markets is positively impacted by both subjective and objective financial literacy.	[44]
5.	Secure privacy	These difficulties are important barriers to the development of financial organizations, and they frequently lead to considerable losses in the form of information, theft, cash loss and other damages.	[62, 80]
6.	Satisfaction	According to the findings, major direct influences on the continuation of m-banking have been identified as perceived ubiquity, considered utility, satisfaction, enabling conditions, perceived security concerns, and trust.	[66, 74, 81]
7.	Positively correlated	In the three different types of interbank networks, authors discover that network entropy is strongly connected with the impact of systemic risk. The network entropy in the small-world network is the highest, followed by those in the random network and the scale-free network.	[46]
8.	Stability	The result of this study use SVM in the banking sector to gain the stability and descriptive power.	[7, 82, 83]
9.	Accuracy	The study shows the outcome of 89% accuracy is achieved in the supervised technique when grouping using the SVM classifier.	[15, 24, 47, 48, 50, 51]
10.	Interconnectedness	Due to an exceptionally high level of interconnection, the stress test demonstrated that the KCB bank hypothetically produced a few contagious defaults.	[32]
11.	Prediction	The data mining technique in proposed like J48 prediction tree enhance the capabilities of cybercrime prediction in the banking sector.	[12]
12.	Operating performance	The findings show that throughout the period, the banking industry steadily improved in all three operational areas, profitability performance, risk management and operating performance.	[52, 75]
13.	Protection	The financial network is severely shaken, and excessive risk will immediately provide protection to the network's defences, explode of systemic risk, and threaten the performance of the banking system through shadow banking.	[9, 84]
14.	Security	The article explains the various security problem and corrective measure are discussed by using the fog clouding, cloud computing AI and ML.	[5, 28, 38, 54, 57, 58, 70, 73, 85-88]
15.	Reliable Efficiency	This article has contributed to the literature on efficiency studies, where it is critical to consider issues of accuracy and bias when assessing efficiency level.	[21, 59, 63]
16.	Safety	The paper provides the safeguard to the money laundering of the virtual currencies.	[24, 33, 89, 90]
17.	Diversification	The findings of this article will have an impact on the global development, expansion, and diversification of Islamic financial services.	[19]
18.	Performance	These studies make use of 10 financial parameters that are roughly divided into four groups to compare the performance of Islamic banking over these two time periods.	[36, 53, 60, 91-93]
19.	Confidence	The impacts are filtered through the user's online confidence and the perceived danger of cybercrime.	[61]
20.	Innovation	The paper aims to assess the effects of more recent technology advancements on the financial services industry and the necessity of maximizing FinTech's potential in the years to come.	[78]
21.	Profitability	A digital euro, depending on how it is made, might increase bank competitiveness and profitability by absorbing a significant amount of idle and excess reserves that encourage bank digitization without restricting lending.	[94]
22.	Awareness	The paper included 16 CMOCs that explained how victimisation was caused by cognitive, social isolation, mental health issues, physical and wealth status and the nature of scams.	[64, 68]
23.	Effectiveness	The purpose of this study to help market players become more effectiveness and cooperative. The challenges brought on by heavy regulation may call for a more flexible and ethical strategy to financial regulation.	[35, 37, 76, 95]
24.	Motivation	The article outlines the actual motivation behind banks' interest in blockchain technology and the challenges they are facing. A qualitative approach was used, and 16 industry specialists were questioned to gain a thorough knowledge of the field.	[72, 96]
25.	Sustainability	In this study, financial performance was compared to sustainability practises from the standpoint of Islamic banking.	[67]

TABLE 7. Enhance the competences of existing system to secure the banking sector.

S. No	Competences to secure the System	Description	References
1.	Access control	This paper suggests the key-revocation procedure for new access control that makes use of blockchain technology for the employs within the banking sector. Despite the customer being authenticated to open banking, customer revoked in accordance with the bank branch's status answer.	[4, 80, 94]
2.	Artificial intelligence	In this article, authors present an artificial intelligence system for creating a model for the prediction of service quality with a focus on the banking industry.	[1, 43, 45, 52, 75, 80, 86]
3.	Security Techniques	In this study, researchers examine the effects of security measures used around user terminals. To protect the security of Internet banking, researcher's categories available security solutions into, financial institution domain, user terminal domain and network domain.	[31, 84]
4.	Crime busting model	Two dynamic ranking algorithms were suggested in this paper's crime-busting model to determine the likelihood of a suspect and the intricacy of a social network and potential for a leader	[97]
5.	Systemic risk	By utilizing Copula to look at how non- domestic systemically domestic systemically important banks significant banks are associated with financial crises occurs, researchers may assess the systemic risk of the whole banking sector.	[9, 34, 47, 53]
6.	Classic domain	The authors constructed the traditional fintech-served real economy domain and node domain as well as the assessment objects of real economy, computed the association between each element affecting development level and evaluated development level, and produced the weight coefficient of each index.	[8]
7.	Fraud Detection	The trials done with actual transaction log files from internet banks point to prudent-based fraud detection as a potential replacement for online banking.	[37, 39, 40, 42, 49-51, 69, 87, 93, 96, 98]
8.	Intelligent hybrid model	This article seeks to an intelligent hybrid model based on multilayer perceptron neural network and fuzzy regression of the impacts of banking on the relative electronic share of banks is created to achieve this goal.	[29, 38]
9.	Moderating effect	This study examines the mediating and moderating effects of rural individuals' objective and subjective financial literateness on the ability to make sound financial decisions.	[80]
10.	Authentication	To preserve high security and authenticity within the financial sectors, these research subjects seek to examine the existing situation from a variety of angles and offer fresh research directions.	[6, 80, 85, 88]
11.	Mixed methods approach	This study examines the future of mobile banking from the standpoint of emerging markets. The study uses a mixed methods technique to illustrate the continuity of m-banking using an integrated model.	[81]
12.	Green Finance	In the paper, the green finance applied in the building up of smart cities.	[77]
13.	KNN Model	Support vector machine in the C SVM classification and K-nearest neighbor (KNN) models are used to identify the cybercriminal and determine the cybercrime information.	[47]
14.	Algorithm	K-means chooses the initial centroids so that the classifier may mine the record and use the J48 algorithm to forecast cybercrimes.	[12, 36, 48, 79]
15.	Network Process structure	A non-performance loan in the network of process structure is built to measure the banks' performance.	[9, 52]
16.	Cloud computing	The paper explains the IoT forensic to investigate the cybercrime in the smart city by using the various technology AI, ML, clouding computing, blockchain and fog computing.	[54, 99]
17.	E-Wallet	This article offers a security analysis of various top Canadian banks' Android e-wallet apps.	[58]
18.	Markov chain	In this article, Markov chains and Bayesian inference are applied to the nature of cybercrime was examined using inference, and the likelihood of it happening, and the outcomes were utilized to based on, examine the likelihood that cybercrimes may occur the elements considered	[24]
19.	Anti-Money laundering	This article examines how anti-money laundering laws and efforts to combat money laundering and the obstacles it poses. bitcoin and other cryptocurrencies	[41, 65, 68, 90, 100]
20.	Packet Inspection	This paper offers an overview of packet inspection, which may be used to identify insiders in cybercrime.	[25]
21.	Thematic analysis	The article intends to investigate how AI may affect Qatari banks' cybersecurity. Nine specialists in Qatar's banking sector were interviewed, and their thematic analysis of their answers	[5]
22.	T-test	The implication of the variable performance between the two periods of time was assessed by the research using a T-test.	[63, 91]
23.	Ad-hoc/ wireless Networking	According to hypothesis, media headlines about cybercrime victims and the avoidance of online social networking, network, shopping, and banking is on the rise.	[61, 102-104]
24.	Knowledge based system	A potential turning point in the quick identification of distinctive and original fraud patterns in Internet banking is presented in this research as a workable substitute for brittleness in knowledge-based systems.	[98]

TABLE 7. *(Continued.)* **Enhance the competences of existing system to secure the banking sector.**

25.	Data Mining	The purpose of this study is to use data mining to uncover the critical factors affecting sukuk ratings.	[17, 92]
26.	Blockchain	In this research authors explore the literature on blockchain-based CBDC schemes and analyze both functional and non-functional needs for CBDC design	[62, 72, 82]
27.	CyberTech	The study investigates whether bank stability is impacted by the rule of diminishing marginal returns from excessive spending on cyber technology.	[83]
28.	RegTech	The paper attempt to interpret banking the regulatory issue in the financial sectors by using financial technology.	[76]
29.	Digital forensics	This article discusses the developing field of digital investigations known as Fintech, which deals with financial technologies. New Fintech is being introduced as a result of society's shift to digital interactions for purchases, money transfers, and other financial activities.	[71, 89]
30.	Digital trends	This article's goals are to outline the various applications of IoT in finance and examine how IoT has affected conventional banks' operational procedures.	[55]
31.	Digital infrastructure	This article suggested banking organizations adopt the required digital technology into their processes to reduce the expenses. To embrace technology in service delivery, they must also invest in digital infrastructure and personnel training.	[95]
32.	Multifactor authentication system	The number of cases of identity theft and fraud-related cybercrime has increased in recent years. To address this issue, this paper implements a multifactor authentication system using an information fusion technique using a fuzzy logic, adaptive neural-fuzzy inference system and ANN.	[30]

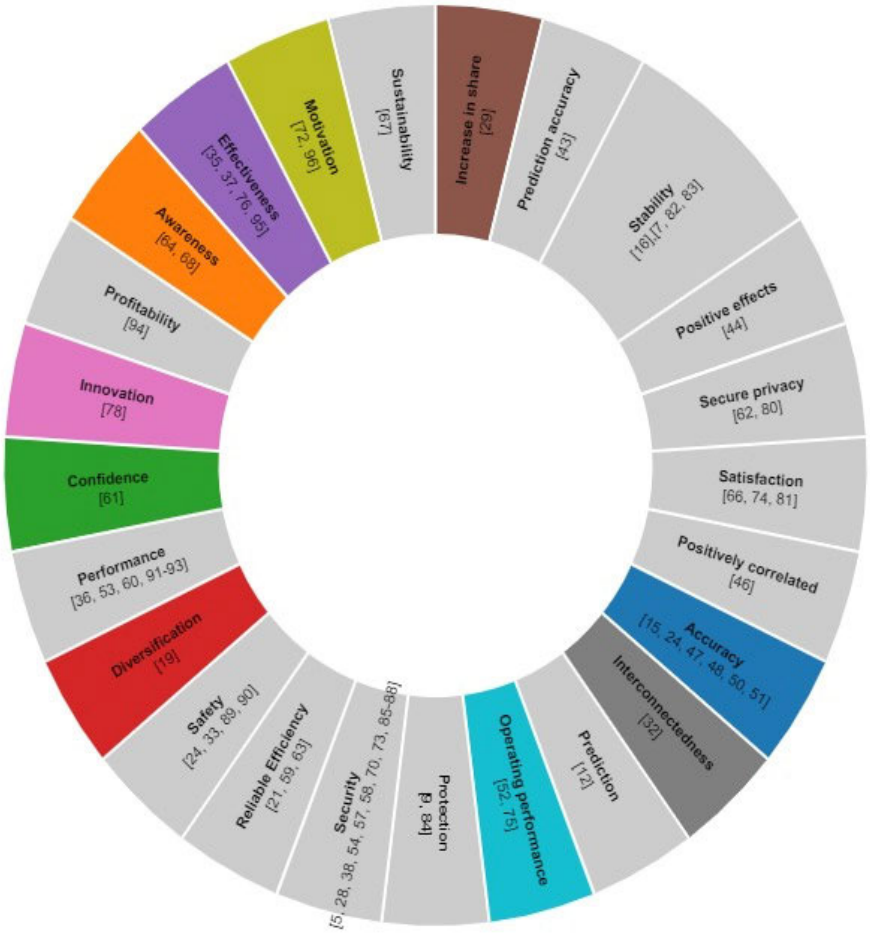


FIGURE 8. **Benefit gained by using AI system.**

The reason of this technology to make the transaction end to end encrypted and provide high security to the existing system and reduce the risk of cybercrime in the financial sector [19], [22], [56], [77]. FinTech Revolution, an acronym for financial technology, is a disruptive innovation that has swept the financial services sector off its feet. It is fueled by

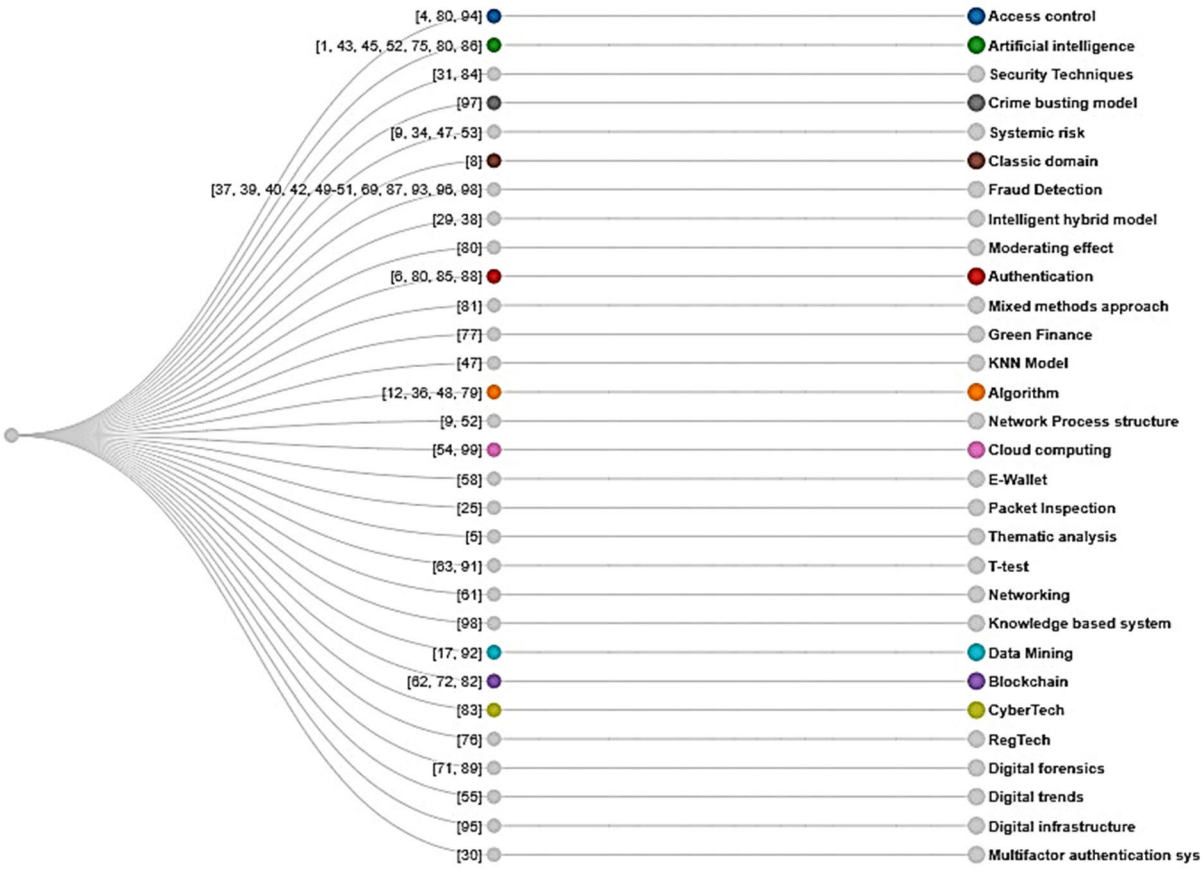


FIGURE 9. Enhance the competences of existing system.

technology and driven by client demand. It is a cutting-edge platform used to create and offer financial services and goods. Cheap mobile data and the quick uptake of smartphones in India are expected to have an influence not just on internet usage patterns but also on general media tastes [78]. A new business model for the financial system is being introduced by FinTech [23], [25], which is dependent on cutting-edge technology like artificial intelligence and big data [52]. In the growth of an advance wave of technological and revolution of industries, Fintech is reshaping the financial sector [79]. Innovative financial services and solutions have a limitless market opportunity thanks to FinTech. The rise of FinTech sector has increased the activity of stock market in the index of FinTech. A new economic form is introduced to the actual economy by FinTech, which is renowned for its enormous development potential and high computing power. The real economy must change and expand, and one of the main forces behind real economic growth is the development of FinTech [8], [43], [44], [63], [80].

RQ 3. What are the key benefits gained by the banking sector using biometric systems after overcoming cyberattacks?

Indirect cybercrime costs are a significant issue for today's Internet-dependent society since they are borne by wary Internet users who are afraid to utilize online services. However, less experienced Internet users considerably perceive risk as being higher and avoid online banking and shopping. The aim of this RQ is to describe the key benefits gained by the banking sectors using biometric system to overcome the risk of cybercrime in the table 6 and figure 8.

RQ 4. Using the literature as evidence, how can we enhance the competence of the existing system to secure the banking sector?

Internet banking services are subject to security violations. Laws governing is playing a significant role in the internet banking services, such as the electronic signature law, have been passed to control these incidents; however, these laws do not, by themselves, prevent such incidents from happening. To address these security issues for the online identity techniques used in the Internet banking service, a variety of security solutions have been investigated. This RQ aim to enhance the competences of banking sector in the existing system to provide high security and authentication which increase the customer satisfaction. Below figure 9 show graphically representation and table 7 show the available system to secure the risk of cybersecurity.

V. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate

on the importance of the work or suggest applications and extensions.

The future of data or cyber security depends on biometrics. To increase security, this article introduces a biometric identification system that may be integrated into any system including computer login, e-commerce, access control and online banking. Although many banking customers are tired of constantly having to provide identification proof, the risk of identity theft will only grow if this practice is abandoned. Due to the rise in internet usage, crime has migrated from the real world to the digital one, making people all over the world more susceptible to it. Criminals are intelligent and imaginative. Wherever there is money to be stolen, clever people will figure out how to do so. Technical abuse has gotten harder over the past ten years as software and hardware manufacturers have focused more on the safety and security of their products, software, and operating systems. In the upcoming years, deep-fakes and other new technological tools will be used to abuse the human target. These are powered by artificial intelligence and will get harder for humans to find. However, this technical development also provides more artefacts of evidence that can be examined to comprehend attacks. This SLR work highlights the below outcome:

- Banks and financial organizations having biometrics security system and tools to detect fraud by using the AI technique.
- Gain information about emerging problems that can be used to create new biometrics verification to protect banking sectors and their customers.
- Understanding the benefits of Fintech crime risks to define and manage cybercrime by utilizing the AI tools in the existing system.
- To take advantage of innovative approaches and strategies to investigate fresh Fintech offences and locate offenders.

Current stakeholder pressure on traditional banking institutions to adopt new technologies is high. Data security, however, cannot be compromised because of the intrinsic nature of this industry. The relationship between banking organizations and their customers requires that users have a high level of trust in their bank branch. Reputation has a direct impact on a bank's performance, capacity to draw in new clients, and capacity to keep hold of current ones. These problems make it difficult to make decisions about how to handle the difficulties of integrating biometrics system, digital transformation, and cybersecurity into the banking sector. So there is a high demand for bank biometric security systems. In their mobile apps, many banks use biometrics like facial recognition, voice recognition and fingerprint scanning. The goal of this study is to create an analysis model that would show how cybercrime, digitalization, and AI could be used to the banking industry and to provide high security and authenticity to the existing system. The analysis is based on four questions: 1) what are the key features of biometrics system that affect banking and prevent cyberattacks. 2) How can cybercrime influence FinTech in the financial and banking sectors. 3) After overcoming the risk of cyberattack, what are the key benefits gained by the banking sector using biometric systems and 4) how we can enhance the competences of existing systems to secure the banking sector from the cybercrime. These questions highlight the current problems faced in the banking industry to secure the banking and financial sectors from cyber-attacks and cybercrime.

IMPLICATIONS

This research has many implications for Islamic and conventional banking and other financial institutions. By using the competencies of biometrics systems in the banking industry, the productivity of different operations will be boosted. Biometrics solutions can resolve the issue of cyber-attacks and minimize the risk of cybercrime to create peace of mind for bank customers by providing a secure atmosphere and building a strong relationship between the client and bank.

REFERENCES

[1] M. Castelli, L. Manzoni, and A. Popovič, "An artificial intelligence system to predict quality of service in banking organizations," *Comput. Intell. Neurosci.*, vol. 2016, May 2016, Art. no. 9139380.

[2] F. Gideon, M. A. Petersen, J. Mukuddem-Petersen, and B. De Waal, "Bank liquidity and the global financial crisis," *J. Appl. Math.*, vol. 2012, May 2012, Art. no. 743656.

[3] L. Sun, S. Wu, Z. Zhu, and A. Stephenson, "Noninterest income and performance of commercial banking in China," *Sci. Program.*, vol. 2017, Feb. 2017, Art. no. 4803840.

[4] K. Riad and M. Elhoseny, "A blockchain-based key-revocation access control for open banking," *Wireless Commun. Mobile Comput.*, vol. 2022, Jan. 2022, Art. no. 3200891.

[5] K. AL-Dosari, N. Fetais, and M. Kucukvar, "Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges," *Cybern. Syst.*, vol. 54, pp. 1–29, 2023.

[6] A. T. Kiyani, A. Lasebae, K. Ali, and M. Ur-Rehman, "Secure online banking with biometrics," in *Proc. Int. Conf. Adv. Emerg. Comput. Technol. (AECT)*, Feb. 2020, pp. 1–6.

[7] S. Li, M. Wang, and J. He, "Prediction of banking systemic risk based on support vector machine," *Math. Problems Eng.*, vol. 2013, May 2013, Art. no. 136030.

[8] M. Zhou and X. Zheng, "Evaluation of the development of FinTech-served real economy based on FinTech improvement," *Discrete Dyn. Nature Soc.*, vol. 2021, Nov. 2021, Art. no. 4836933.

[9] H. Pan and H. Fan, "The stability of banking system with shadow banking on different interbank network structures," *Discrete Dyn. Nature Soc.*, vol. 2021, Apr. 2021, Art. no. 6650327.

[10] P. Suja and N. Raghavan, "Cybercrime in banking sector," *Int. J. Res. Social Sci.*, vol. 4, no. 1, pp. 189–194, 2014.

[11] A. Raghavan and L. Parthiban, "The effect of cybercrime on a bank's finances," *Int. J. Current Res. Academic Rev.*, vol. 2, no. 2, pp. 173–178, 2014.

[12] K. C. Lekha and S. Prakasam, "Data mining techniques in detecting and predicting cyber crimes in banking sector," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 1639–1643.

[13] L. Ali, "Cyber crimes—A constant threat for the business sectors and its growth (a study of the online banking sectors in GCC)," *J. Developing Areas*, vol. 53, no. 1, pp. 267–279, 2019.

[14] M. Button and J. Whittaker, "Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation," *Int. J. Law, Crime Justice*, vol. 66, Sep. 2021, Art. no. 100482.

[15] Warjiyono, S. Aji, Fandhilah, N. Hidayatun, H. Faqih, and Liesnaningsih, "The sentiment analysis of FinTech users using support vector machine and particle swarm optimization method," in *Proc. 7th Int. Conf. Cyber IT Service Manage. (CITSM)*, vol. 7, Nov. 2019, pp. 1–5.

[16] V. Stefanenko, D. Savenko, and H. Penikas, "Evaluating the 2013 Islamic banking regulation capital reform implication for the valuation of the Islamic banks," in *Proc. Int. Conf. Sustain. Islamic Bus. Finance*, Dec. 2021, pp. 14–19.

[17] M. Kartiwi, T. Arundina, M. A. Omar, and T. S. Gunawan, "S-Rater: Data mining application in Islamic financial sector," in *Proc. 5th Int. Conf. Inf. Commun. Technol. Muslim World (ICT4M)*, Nov. 2014, pp. 1–5.

[18] A. S. B. A. Latiff, "The need for an information system for the dissemination of knowledge on Islamic banking," in *Proc. 5th Int. Conf. Inf. Commun. Technol. Muslim World (ICT4M)*, Mar. 2013, pp. 1–5.

[19] M. Majdalawieh, F. Marir, and I. Tiemsani, "Developing adaptive Islamic law business processes models for Islamic finance and banking by text mining the holy Qur'an and Hadith," in *Proc. IEEE 15th Int. Conf. Dependable, Autonomic Secure Comput., 15th Int. Conf. Pervasive Intell. Comput., 3rd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Nov. 2017, pp. 1278–1283.

[20] I. Saba, R. Kouser, and I. S. Chaudhry, "FinTech and Islamic finance-challenges and opportunities," *Rev. Econ. Develop. Stud.*, vol. 5, no. 4, pp. 581–890, 2019.

[21] S. Zakaria, M. I. Salleh, and S. Hassan, "A bootstrap data envelopment analysis (BDEA) approach in Islamic banking sector: A method to strengthen efficiency measurement," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, Dec. 2014, pp. 657–661.

[22] M. Hanif, "Differences and similarities in Islamic and conventional banking," *Int. J. Bus. Social Sci.*, vol. 2, no. 2, pp. 1–25, Apr. 2014.

[23] M. R. Rabbani, Y. Abdulla, A. Basahr, S. Khan, and M. A. M. Ali, "Embracing of FinTech in Islamic finance in the post COVID era," in *Proc. Int. Conf. Decis. Aid Sci. Appl. (DASA)*, Nov. 2020, pp. 1230–1234.

[24] Q.-A. Kester and E. J. Afoma, "Crime predictive model in cybercrime based on social and economic factors using the Bayesian and Markov theories," in *Proc. Int. Conf. Comput., Comput. Model. Appl. (ICCMA)*, Jul. 2021, pp. 165–170.

[25] D.-Y. Kao, "Cybercrime countermeasure of insider threat investigation," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 413–418.

[26] S. Roksandic, N. Protrka, and M. Engelhart, "Trustworthy artificial intelligence and its use by law enforcement authorities: Where do we stand?" in *Proc. 45th Jubilee Int. Conv. Inf., Commun. Electron. Technol. (MIPRO)*, May 2022, pp. 1225–1232.

[27] J. Rajamäki, J. Tervahartiala, S. Tervola, S. Johansson, L. Ovaska, and P. Rathod, "How transparency improves the control of law enforcement authorities' activities?" in *Proc. European Intell. Secur. Inform. Conf.*, Aug. 2012, pp. 14–21.

[28] M. Antonescu and R. Birău, "Financial and non-financial implications of cybercrimes in emerging countries," *Proc. Econ. Finance*, vol. 32, pp. 618–621, Jan. 2015.

[29] Z. Ghasemi, M. A. Kermani, and T. Allahviranloo, "Exploring the main effect of e-Banking on the banking industry concentration degree on predicting the future of the banking industry: A case study," *Adv. Fuzzy Syst.*, vol. 2021, Aug. 2021, Art. no. 8856990.

[30] J. Phiri, T.-J. Zhao, C. H. Zhu, and J. Mbale, "Using artificial intelligence techniques to implement a multifactor authentication system," *Int. J. Comput. Intell. Syst.*, vol. 4, no. 4, pp. 420–430, Jun. 2011.

[31] K. Lee, S.-Y. Lee, and K. Yim, "Classification and analysis of security techniques for the user terminal area in the Internet banking service," *Secur. Commun. Netw.*, vol. 2020, Jun. 2020, Art. no. 7672941.

[32] H. Fan, A. A. L. L. Amalia, and Q. Q. Gao, "The assessment of systemic risk in the Kenyan banking sector," *Complexity*, vol. 2018, Jan. 2018, Art. no. 8767836.

[33] S. Azmat, A. S. M. S. Azad, H. Ghaffar, A. Hayat, and A. Chazi, "Conventional vs Islamic banking and macroeconomic risk: Impact on asset price bubbles," *Pacific–Basin Finance J.*, vol. 62, Sep. 2020, Art. no. 101351.

[34] Y. Chen, Y. Shi, X. Wei, and L. Zhang, "Domestic systemically important banks: A quantitative analysis for the Chinese banking system," *Math. Problems Eng.*, vol. 2014, Mar. 2014, Art. no. 819371.

[35] I. K. Ofori, C. Quaidoo, and P. E. Ofori, "What drives financial sector development in Africa? Insights from machine learning," *Appl. Artif. Intell.*, vol. 35, no. 15, pp. 2124–2156, Dec. 2021.

[36] K. R. Shanmugam and R. Nigam, "Impact of technology on the financial performance of Indian commercial banks: A clustering based approach," *Innov. Develop.*, vol. 10, no. 3, pp. 433–449, Sep. 2020.

[37] A. Singh, R. K. Ranjan, and A. Tiwari, "Credit card fraud detection under extreme imbalanced data: A comparative study of data-level algorithms," *J. Exp. Theor. Artif. Intell.*, vol. 34, no. 4, pp. 571–598, Jul. 2022.

[38] R. R. Patil, G. Kaur, H. Jain, A. Tiwari, S. Joshi, K. Rao, and A. Sharma, "Machine learning approach for phishing website detection: A literature survey," *J. Discrete Math. Sci. Cryptograp.*, vol. 25, pp. 817–827, 2022.

[39] V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," *Proc. Comput. Sci.*, vol. 165, pp. 631–641, 2019.

[40] J. Domashova and E. Kripak, "Identification of non-typical international transactions on bank cards of individuals using machine learning methods," *Proc. Comput. Sci.*, vol. 190, no. 3, pp. 178–183, 2021.

[41] J. Domashova and N. Mikhailina, "Usage of machine learning methods for early detection of money laundering schemes," *Proc. Comput. Sci.*, vol. 190, pp. 184–192, Jan. 2021.

[42] J. Nicholls, A. Kuppa, and N.-A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," *IEEE Access*, vol. 9, pp. 163965–163986, 2021.

[43] C. Liu, Y. Fan, and X. Zhu, "FinTech index prediction based on RF-GA-DNN algorithm," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–9, Jun. 2021.

[44] Y. Li, Z. Li, F. Su, Q. Wang, and Q. Wang, "FinTech penetration, financial literacy, and financial decision-making: Empirical analysis based on tar," *Complexity*, vol. 2020, Dec. 2020, Art. no. 3950981.

[45] A. R. D. Rodrigues, F. A. F. Ferreira, F. J. C. S. N. Teixeira, and C. Zopounidis, "Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework," *Res. Int. Bus. Finance*, vol. 60, Apr. 2022, Art. no. 101616.

[46] L. He and S. Li, "Network entropy and systemic risk in dynamic banking systems," *Complexity*, vol. 2017, Nov. 2017, Art. no. 1852897.

[47] K. Veena, K. Meena, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "*C* SVM classification and KNN techniques for cyber crime detection," *Wireless Commun. Mobile Comput.*, vol. 2022, Jan. 2022, Art. no. 3640017.

[48] P. Kumar and F. Iqbal, "Credit card fraud identification using machine learning approaches," in *Proc. 1st Int. Conf. Innov. Inf. Commun. Technol. (ICIICT)*, Apr. 2019, pp. 1–4.

[49] N. Rtayli and N. Enneya, "Selection features and support vector machine for credit card risk identification," *Proc. Manuf.*, vol. 46, pp. 941–948, Jan. 2020.

[50] O. Adepoju, J. Wosowei, and H. Jaiman, "Comparative evaluation of credit card fraud detection using machine learning techniques," in *Proc. Global Conf. Advancement Technol. (GCAT)*, Oct. 2019, pp. 1–6.

[51] A. Mehbodniya, I. Alam, S. Pande, R. Neware, K. P. Rane, M. Shabaz, and M. V. Madhavan, "Financial fraud detection in healthcare using machine learning and deep learning techniques," *Secur. Commun. Netw.*, vol. 2021, Sep. 2021, Art. no. 9293877.

[52] D.-Y. Liu, Y.-C. Wu, C.-H. Lin, and W.-M. Lu, "The effects of nonperforming loans on dynamic network bank performance," *Discrete Dyn. Nature Soc.*, vol. 2017, Jun. 2017, Art. no. 9458315.

[53] H. A. Al-Shari and M. A. Lokhande, "The relationship between the risks of adopting FinTech in banks and their impact on the performance," *Cogent Bus. Manage.*, vol. 10, no. 1, Dec. 2023, Art. no. 2174242.

[54] S. Rani, A. Kataria, V. Sharma, S. Ghosh, V. Karar, K. Lee, and C. Choi, "Threats and corrective measures for IoT security with observance of cybercrime: A survey," *Wireless Commun. Mobile Comput.*, vol. 2021, Apr. 2021, Art. no. 5579148.

[55] F. Khanboubi, A. Boulmakoul, and M. Tabaa, "Impact of digital trends using IoT on banking processes," *Proc. Comput. Sci.*, vol. 151, pp. 77–84, May 2019.

[56] G. Singh, R. Gupta, and V. Vatsa, "A framework for enhancing cyber security in FinTech applications in India," in *Proc. Int. Conf. Technol. Advancement Innov. (ICTAI)*, Nov. 2021, pp. 274–279.

[57] E.-L. Nawa, M. Chitauro, and F. B. Shava, "Assessing patterns of cybercrimes associated with online transactions in Namibia banking institutions' cyberspace," in *Proc. 3rd Int. Multidisciplinary Inf. Technol. Eng. Conf. (IMITEC)*, Nov. 2021, pp. 1–6.

[58] R. Kaur, Y. Li, J. Iqbal, H. Gonzalez, and N. Stakhanova, "A security assessment of HCE-NFC enabled e-wallet banking Android apps," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 492–497.

[59] R. Carvalho, M. Goldsmith, and S. Creese, "Applying semantic technologies to fight online banking fraud," in *Proc. Eur. Intell. Secur. Informat. Conf.*, Sep. 2015, pp. 61–68.

[60] D. Caragea, M. Chen, T. Cojoianu, M. Dobri, K. Glandt, and G. Mihaila, "Identifying FinTech innovations using BERT," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 1117–1126.

[61] M. Riek, R. Bohme, and T. Moore, "Measuring the influence of perceived cybercrime risk on online service avoidance," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2, pp. 261–273, Mar. 2016.

[62] C. Gomathi and K. Jayasri, "Rain drop service and biometric verification based blockchain technology for securing the bank transactions from cyber crimes using weighted fair blockchain (WFB) algorithm," *Cybern. Syst.*, vol. 54, no. 4, pp. 550–576, Jul. 2022.

[63] A. Wahab, T. M. Alam, and M. M. Raza, "Usability evaluation of FinTech mobile applications: A statistical approach," in *Proc. Int. Conf. Innov. Comput. (ICIC)*, Nov. 2021, pp. 1–10.

[64] A. Burton, C. Cooper, A. Dar, L. Mathews, and K. Tripathi, "Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review," *Exp. Gerontol.*, vol. 159, Mar. 2022, Art. no. 111678.

[65] D. S. Demetis, "Fighting money laundering with technology: A case study of Bank X in the U.K.," *Decis. Support Syst.*, vol. 105, pp. 96–107, Jan. 2018.

[66] M. Muflih, "The link between corporate social responsibility and customer loyalty: Empirical evidence from the Islamic banking industry," *J. Retailing Consum. Services*, vol. 61, Jul. 2021, Art. no. 102558.

[67] A. Jan, M. Marimuthu, and M. P. B. M. M. Isa, "The nexus of sustainability practices and financial performance: From the perspective of Islamic banking," *J. Cleaner Prod.*, vol. 228, pp. 703–717, Aug. 2019.

[68] M. E. Lokanan, "Predicting money laundering using machine learning and artificial neural networks algorithms in banks," *J. Appl. Secur. Res.*, pp. 1–25, Aug. 2022.

[69] D. Dighe, S. Patil, and S. Kokate, "Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study," in *Proc. 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Aug. 2018, pp. 1–6.

[70] J. M. Marqués et al., "Policy report on FinTech data gaps," *Latin Amer. J. Central Banking*, vol. 2, no. 3, Sep. 2021, Art. no. 100037.

[71] B. Nikkel, "FinTech forensics: Criminal investigation and digital evidence in financial technologies," *Forensic Sci. Int., Digit. Invest.*, vol. 33, Jun. 2020, Art. no. 200908.

[72] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees," *Technol. Forecasting Social Change*, vol. 158, Sep. 2020, Art. no. 120166.

[73] A. Nasir, N. Jan, D. Pamucar, and S. U. Khan, "Analysis of cybercrimes and security in FinTech industries using the novel concepts of interval-valued complex q-rung orthopair fuzzy relations," *Expert Syst. Appl.*, vol. 224, Aug. 2023, Art. no. 119976.

[74] X. Chen, X. You, and V. Chang, "FinTech and commercial banks' performance in China: A leap forward or survival of the fittest?" *Technol. Forecasting Social Change*, vol. 166, May 2021, Art. no. 120645.

[75] M. Doumpos, C. Zopounidis, D. Gounopoulos, E. Platanakis, and W. Zhang, "Operational research and artificial intelligence methods in banking," *Eur. J. Oper. Res.*, vol. 306, no. 1, pp. 1–16, Apr. 2023.

[76] I. Anagnostopoulos, "FinTech and RegTech: Impact on regulators and banks," *J. Econ. Bus.*, vol. 100, pp. 7–25, Nov. 2018.

[77] Z. He, Z. Liu, H. Wu, X. Gu, Y. Zhao, and X. Yue, "Research on the impact of green finance and FinTech in smart city," *Complexity*, vol. 2020, Dec. 2020, Art. no. 6673386.

[78] A. Mehrotra and S. Menon, "Second round of FinTech—Trends and challenges," in *Proc. 2nd Int. Conf. Comput., Autom. Knowl. Manage. (ICCAKM)*, Jan. 2021, pp. 243–248.

[79] A. S. Sadiq, A. A. Dehkordi, S. Mirjalili, J. Too, and P. Pillai, "Trustworthy and efficient routing algorithm for IoT-FinTech applications using nonlinear Lévy Brownian generalized normal distribution optimization," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2215–2230, Feb. 2023.

[80] H. U. Khan, M. Z. Malik, M. K. B. Alomari, S. Khan, A. A. S. A. Al-Maadid, M. K. Hassan, and K. Khan, "Transforming the capabilities of artificial intelligence in GCC financial sector: A systematic literature review," *Wireless Commun. Mobile Comput.*, vol. 2022, Apr. 2022, Art. no. 8725767.

[81] I. Hidayat-ur-Rehman, A. Ahmad, M. N. Khan, and S. A. Mokhtar, "Investigating mobile banking continuance intention: A mixed-methods approach," *Mobile Inf. Syst.*, vol. 2021, Sep. 2021, Art. no. 9994990.

[82] T. Zhang and Z. Huang, "Blockchain and central bank digital currency," *ICT Exp.*, vol. 8, no. 2, pp. 264–270, Jun. 2022.

[83] M. H. Uddin, S. Mollah, and M. H. Ali, "Does cyber tech spending matter for bank stability?" *Int. Rev. Financial Anal.*, vol. 72, Nov. 2020, Art. no. 101587.

[84] T. A. Hemphill and P. Longstreet, "Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards," *Technol. Soc.*, vol. 44, pp. 30–38, Feb. 2016.

[85] A. Bani-Hani, M. Majdalweieh, and A. AlShamsi, "Online authentication methods used in banks and attacks against these methods," *Proc. Comput. Sci.*, vol. 151, pp. 1052–1059, 2019.

[86] A. Mahmud, "Application and criminalization of artificial intelligence in the digital society: Security threats and the regulatory challenges," *J. Appl. Secur. Res.*, vol. 18, no. 1, pp. 1–15, Jan. 2023.

[87] A. Demiriz and B. Ekizoglu, "Using location aware business rules for preventing retail banking frauds," in *Proc. 1st Int. Conf. Anti-Cybercrime (ICACC)*, Nov. 2015, pp. 1–6.

[88] K. K. Lakshmi, H. Gupta, and J. Ranjan, "UPI based mobile banking applications—Security analysis and enhancements," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 1–6.

[89] E. Casey, "The chequered past and risky future of digital forensics," *Austral. J. Forensic Sci.*, vol. 51, no. 6, pp. 649–664, Nov. 2019.

[90] T. S. Sobh, "An intelligent and secure framework for anti-money laundering," *J. Appl. Secur. Res.*, vol. 15, no. 4, pp. 517–546, Oct. 2020.

[91] N. A. Kadir, N. L. Abdullah, N. Harun, N. A. Nordin, and A. Jaffar, "Financial performance of Islamic bank in Malaysia during and after economic crisis," in *Proc. IEEE Colloq. Humanities, Sci. Eng.*, Dec. 2011, pp. 839–844.

[92] T. D. Le, T. H. Ho, D. T. Nguyen, and T. Ngo, "A cross-country analysis on diversification, Sukuk investment, and the performance of Islamic banking systems under the COVID-19 pandemic," *Heliyon*, vol. 8, no. 3, Mar. 2022, Art. no. e09106.

[93] N. C. Roy and S. Prabhakaran, "Insider employee-led cyber fraud (IECF) in Indian banks: From identification to sustainable mitigation planning," *Behaviour Inf. Technol.*, pp. 1–31, Mar. 2023.

[94] P. Fegatelli, "A central bank digital currency in a heterogeneous monetary union: Managing the effects on the bank lending channel," *J. Macroecon.*, vol. 71, Mar. 2022, Art. no. 103392.

[95] D. Agyapong, "Implications of digital economy for financial institutions in Ghana: An exploratory inquiry," *Transnational Corp. Rev.*, vol. 13, no. 1, pp. 51–61, Jan. 2021.

[96] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation," *Cogent Econ. Finance*, vol. 11, no. 1, Dec. 2023, Art. no. 2153412.

[97] Y. Cao, X. Xu, and Z. Ye, "Crime busting model based on dynamic ranking algorithms," *Abstract Appl. Anal.*, vol. 2013, Jul. 2013, Art. no. 308675.

[98] O. O. Maruatona, P. Vamplew, and R. Dazeley, "Prudent fraud detection in Internet banking," in *Proc. 3rd Cybercrime Trustworthy Comput. Workshop*, Oct. 2012, pp. 60–65.

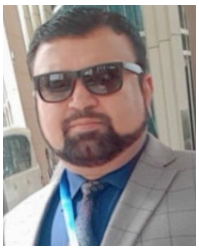
[99] S. M. Hussain, A. Wahid, M. A. Shah, A. Akhunzada, F. Khan, N. U. Amin, S. Arshad, and I. Ali, "Seven pillars to achieve energy efficiency in high-performance computing data centers," in *Recent Trends and Advances in Wireless and IoT-enabled Networks*. London, U.K.: Springer, 2019, pp. 93–105.

[100] S. Mabunda, "Cryptocurrency: The new face of cyber money laundering," in *Proc. Int. Conf. Adv. Big Data, Comput. Data Commun. Syst. (icABCD)*, Aug. 2018, pp. 1–6.

[101] M. Junger, L. Montoya, P. Hartel, and M. Heydari, "Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (Cyber SA)*, Jun. 2017, pp. 1–8.

[102] F. Khan, A. W. Khan, K. Shah, I. Qasim, and A. Habib, "An algorithmic approach for core election in mobile ad-hoc network," *J. Internet Technol.*, vol. 20, no. 4, pp. 1099–1111, 2019.

[103] M. S. Al-kahtani, F. Khan, and W. Taekeun, "Application of Internet of Things and sensors in healthcare," *Sensors*, vol. 22, no. 15, p. 5738, Jul. 2022.
[104] F. Khan, A. W. Khan, S. Khan, I. Qasim, and A. Habib, "A secure core-assisted multicast routing protocol in mobile ad-hoc network," *J. Internet Technol.*, vol. 21, no. 2, pp. 375–383, 2020.



HABIB ULLAH KHAN received the Ph.D. degree in management information systems from Leeds Beckett University, U.K., in 2008. He has nearly 20 years of industry, teaching, and research experience. He is currently a Professor of MIS with the Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Qatar. His research interests include IT adoption, social media, internet addiction, mobile commerce, computer-mediated communication, IT outsourcing, big data, and IT security.

MUHAMMAD ZAIN MALIK received the M.S. degree in business administration from the National University of Modern Languages, Islamabad. From 2011 to 2021, he served in various multinational and national organizations, including FujiFilm, British Council, Ufone, and Jubilee General Insurance Company. In 2015, he joined the Institute of Banking and Finance, Bahauddin Zakaria University, Multan, Pakistan, as a Visiting Lecturer. Since September 2021, he has been a Researcher with the Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar. He has several research articles in international conferences and journals. His research interests include artificial intelligence, blockchain technology, and the implementation of technology in corporate governance.

SHAH NAZIR (Member, IEEE) received the Ph.D. degree in computer science from the University of Peshawar, Pakistan, in December 2015, with a specialization in Software Engineering. He is currently working as an Assistant Professor and Head of the Department at the University of Swabi, Pakistan. Prior to this, he worked at the University of Peshawar, Pakistan, from 2009 to 2016, and received several awards. He has more than 180 research publications in well-reputed international journals and conference proceedings. He is an academic editor of two journals and he is working as a member of the technical committee for more than 140 journals and conferences. He organized one international conference and remains session chair for several conferences. He completed two research projects for the Higher Education Commission of Pakistan. His research interests include component-based software engineering, software birthmark, systematic literature review, big data, and decision-making.

FAHEEM KHAN received the Ph.D. degree in computer science from the University of Malakand, Khyber Pakhtunkhwa, Pakistan. He was an Assistant Professor in Pakistan for four years and supervised many papers and students. Since April 2021, he has been an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include computer networking, wireless networking, MANET, sensor networking, the IoT, artificial intelligence, and AI in healthcare systems.