

Review Article

Transforming the Capabilities of Artificial Intelligence in GCC Financial Sector: A Systematic Literature Review

Habib Ullah Khan ¹, **Muhammad Zain Malik**,¹ **Mohammad Kamel Bader Alomari**,¹ **Sulaiman Khan** ¹, **Alanoud Ali S. A. Al-Maadid**,² **Mostafa Kamal Hassan**,¹ and **Khaliquzzaman Khan**³

¹Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar

²Department of Finance and Economics, College of Business and Economics, Qatar University, Doha, Qatar

³College of Business Administration, American University in the Emirates, Dubai, UAE

Correspondence should be addressed to Habib Ullah Khan; habib.khan@qu.edu.qa

Received 30 January 2022; Revised 4 March 2022; Accepted 21 March 2022; Published 5 April 2022

Academic Editor: Md. Shamsul Huda

Copyright © 2022 Habib Ullah Khan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The publication of this article was funded by Qatar National Library.

Identity and access management is a business process framework that makes it easier to maintain genuine user identities and regulate access to sensitive assets. The word “access control” refers to an organization’s policy for authorizing access procedures, the mechanisms that implement and enforce the policy, and the model that the policy and procedures are built on. Adopting new technology may give rise to specific cyber threats that decrease or degrade business operations. The paper has designed to discuss the artificial intelligence-based access control system as a necessary component of governing and safeguarding the financial sector’s information assets in the Gulf Cooperation Council (GCC) region. Due to the dynamic and complicated nature of security rules for access control, organizations that employ web-enabled remote access in conjunction with applications access deployed over several networks face various obstacles, including increased operational complexity and monitoring concerns. Organizations spend a vast budget on securing their business. As the industry trend has shifted to intelligent internet-based companies on the same side, the cyber threat has become a challenge for the researcher to find the solution. A systematic research is conducted to fill the gaps in the existing literature by picking the most relevant research papers (126) from the four most reputable online repositories based on the four research questions specified. These research topics aim to evaluate the current situation from many perspectives and provide new avenues for future study to be studied soon to maintain high security and authenticity inside financial sectors of the GCC’s countries.

1. Introduction

Human involvement and technological advancements have paved the road for prosperity in human life [1]. Individuals use the Internet as a communication tool to cooperate, communicate, and express their opinions about numerous topics and obtain information and use various technologies such as cell phones and other gadgets [2]. The Internet of Things (IoT) is a new technology that will transform the Internet age over the next several years. Digitally connected factories, facility management, production flow management, inventory management, safety, security, health care, logistics, supply chain optimization, and other industries may all benefit

from IoT [3]. Information systems and smart Internet of things- (IoT-) based solutions have enriched our lives by offering several state-of-the-art applications in various fields, including healthcare, navigation, tracking, smart security, smart homes, smart buildings [4], and smart appliance management systems. Transportation, healthcare [5], the house, entertainment, and other daily activities have all been altered by IoT-based applications [6]. Al-Azawi et al. [7] compared several AI-assisted cybersecurity solutions. The digital age changed business paradigms by allowing businesses to join the market with specific financial advantages [8]. Mobile information systems will continue to function as facilitators of innovation and will support entrepreneurship in

sustainable ways throughout the world [9]. Because of the proliferation of portable devices and the availability of the Internet, mobile learning (M-learning) has exploded in popularity in recent years. The success stories of next generation mobile information systems have been supplemented by the usage of this unique technology in learning and training [10].

Due to the unpredictability of the economic climate and fierce competition, even the well-run businesses are vulnerable to failure and financial disaster. So, whether financial difficulty in publicly traded firms can be projected properly and quickly is dependent on the development of the company, the interest of various investors, and the capital market order [11]. Organizations are interested in altering their company operations and incorporating computer-assisted technologies to serve their clientele [12]. Criminal activity is rising in our society daily. A huge number of threats and acts of violence occur in the community due to this exponential growth. People require security systems and improved living conditions to provide serenity to their lives and raise their living standards. As new technology evolves, it harms the globe in the form of cyber-attacks [13]. Organizations and individuals must endure harmful damage and cyber-attacks on their information systems. Any firm must take security action based on risk assessments in every period of information system modernization. There are other risk analysis approaches to choose from, but the qualitative method is the most effective. The qualitative approach helps the company to make timely decisions about information security [14]. Farooq and Otaibi [15] gave a paper at a symposium on reducing security risks in information systems. Information system security risk management is critical to an organization's commercial performance (ISSRM). The ISSRM ensures privacy, data security, and consistency.

Artificial intelligence (AI) is defined as "the practice of making machines intelligent, with intelligence being the attribute that allows an entity to function correctly and predictably in its environment." Artificial intelligence (AI) is the capacity of a machine to work intelligently by accurately reading incoming inputs and applying these teachings to achieve defined objectives and activities via a flexible design [16]. It is a result of human intelligence. AI is the intelligent base software that focuses on various human intelligence systems compound operations such as image processing, decision-making, speech recognition, and language processing. AI is a fictional technology that has altered many aspects of our life, including transportation, health, marketing, banking, and shopping [17]. In this industrial revolution, artificial intelligence (AI) is playing a key role. It can guard against cyber-attacks, viruses, and illegal access to the information system. AI can help with a variety of cybersecurity challenges. Multiple AI approaches, such as deep learning, machine learning, and concept of knowledge, can be used to reduce the cyber threat [7].

Due to the unpredictability of the economic climate and fierce competition, even the well-run businesses are vulnerable to failure and financial disaster. So whether financial difficulty in publicly traded firms can be projected properly and quickly is dependent on the development of the company,

the interest of various investors, and the capital market order. Many investigators used AI to strengthen the security of information systems and interconnected devices in order to overcome security concerns and dangers. AI approaches assist machines in solving key issues in the same way that people do. AI can detect a variety of dangerous threats and assaults that can affect an organization's system. Using machine learning and deep knowledge, AI approaches respond in real time to numerous threats on the information system. Machine learning is a form of artificial intelligence that assists in identifying the ornament contained in incoming data [17].

Meanwhile, AI is being imposed on the education industry by the rapid advancement of information technology. Educational companies introduced the individual adaptive learning system (IALP) to support student enrolment and probe. It aims to aided teaching system, personalized learning that creates the classroom environment management, individual evaluation, and institute administration system to support the student enrolment and probe [18]. Rapidly changing needs, wants, and behavior of customers are influencing world economics, financial institutions, countries, the budget deficit, and business profitability and revenue aspects, while another view of economic development and financial crises, rapidly changing needs, wants, and behaviors of customers are influencing world economics, financial institutes, countries, and the budget deficit. Thuraisingham discussed the effects of robots and artificial intelligence on corporate economics and potential future study topics [19]. The technique and analysis of business trends and projections concerning sales, income, profits, and expenditures are all part of business forecasting. The goal of business forecasting is to give relevant data based on prophecy. Many businesses must gather this data in order to achieve their objectives [20]. The following are the main contribution of this systematic analysis:

- (i) For recognizing the difficulties facing or faced by financial sector of GCC region most typically
- (ii) To describe many strategies offered to address these difficulties, as well as where these solutions fall short
- (iii) How artificial intelligence-based solutions have been used to handle these problems and how they may be enhanced to ensure high levels of security and authenticity, and
- (iv) To identify the social and economical importance of AI on our lives and other government and nongovernment organizations
- (v) Based on this systematic analysis, new research directions must be proposed to ensure the safety and security of the organizations for both employees and employers

The rest of the paper is organized as follows. Section 2 represents the background study, while Section 3 outlines the systematic protocol followed for this assessment work. Section 4 details the assessment criteria followed for

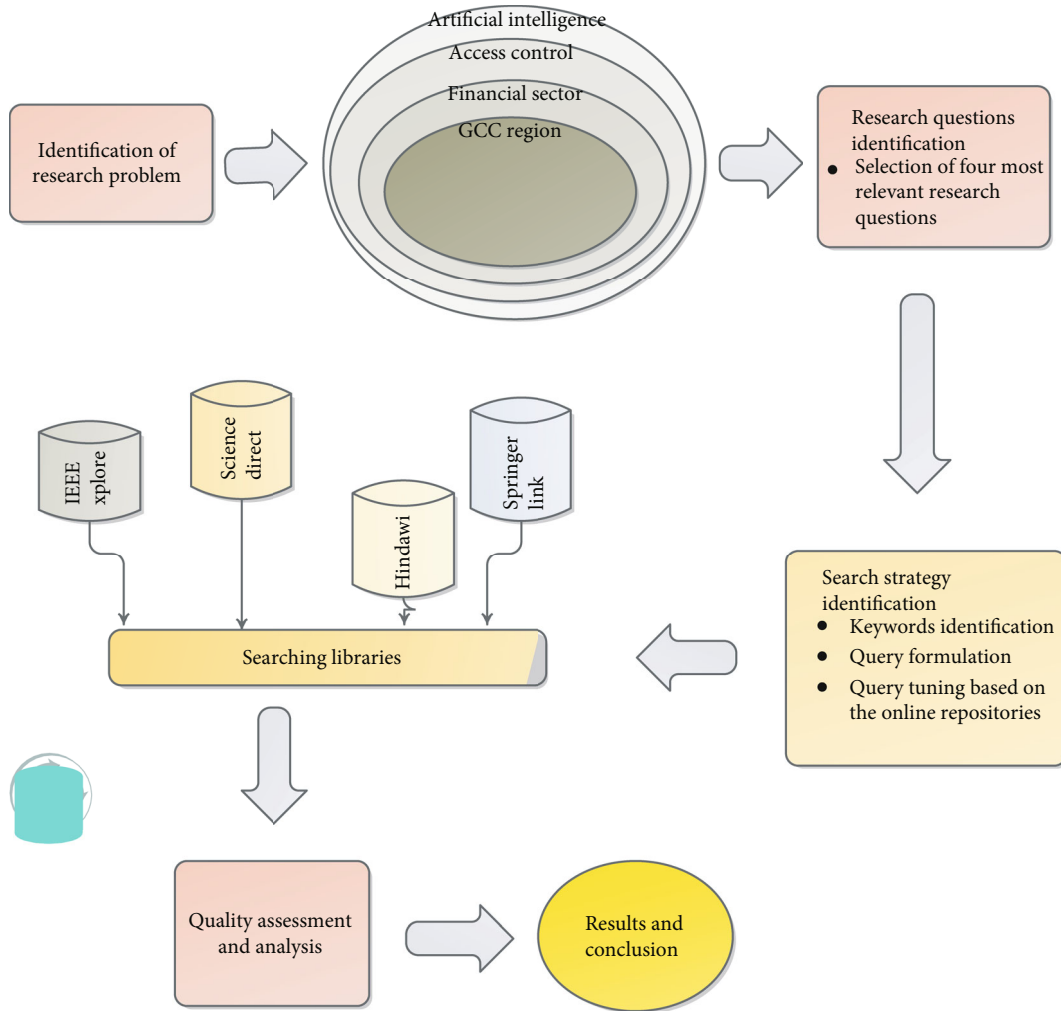


FIGURE 1: Proposed systemic literature review research procedure.

TABLE 1: Research questions.

S. no	Research questions	Description
RQ1.	What are the various types of organizational security risks faced by employees working within the GCC region?	This question primarily focuses on extracting the information regarding different types of security issues most commonly faced by the employees and the people residing in the GCC region.
RQ2.	By utilizing AI capabilities as evidence, how many proactive approaches are proposed to counter organizational security risks in the GCC region?	The primary goal of this research question is to compile a list of various AI-based strategies that have been created to reduce organizational safety and security concerns in the GCC region. In addition, this inquiry aims to provide a new research direction for improving the capabilities of existing models or developing a new upgraded model.
RQ3.	Based on the extant findings, how can we improve the capabilities of the available authentication systems in the GCC organizations?	Based on the literature, this research topic aims to increase the organization’s ability to improve the existing authentic systems to assure high security and ethnicity in GCC-based organizations.
RQ4.	What are the social and economic impacts of AI on financial bodies operating in the GCC region?	AI has a significant impact all around the world. This research topic aims to demonstrate the social and economic effects of AI-based solutions in the financial sectors of the GCC region.

evaluation purposes. Section 5 briefly explains the results and discussion section. Section 6 presents the limitations of this research work followed by the conclusion in Section 7 of the paper.

2. Background Study

Artificial intellect (AI) is a new scientific technology that may simulate and expand human intelligence technology applications. AI is a study area at the crossroads of social science, natural science, and technological science. AI can process information in a way that is akin to human thinking and awareness. AI employs a procedural way to develop and extend the core of intelligence, resulting in a new sort of intelligent computer that behaves similarly to humans. The researchers investigated the influence and impact of AI on stakeholders, consumers, and businesses in the industry to improve the business [1]. Artificial intelligence (AI) has become a danger to people who labour manually as new information technology has been implemented. This danger exists for financial institutions as well. Despite this, investment in AI FinTech has not slowed due to the uncertainty that AI provides to mandatory customers, operators, and financial controllers. AI offers various social benefits to increase its credibility in financial institutions and win public acceptance [2].

Small enterprises contribute significantly to a country's economy. Almost 98 percent of businesses in the United States are small businesses with less than 100 employees. These companies employ a total of 36% of the workforce. It represents a market sector eager to improve its businesses using modern information technologies [3]. Because of blockchain technology, corporate governance has taken a new direction. A reliable and effective GITS (global information transmission system) will require a reliable value to the transmission system, the cornerstone of blockchain technology. A reliable and effective GITS (global information transmission system) will require a reliable deal to the transmission system, the cornerstone of blockchain technology. By employing cryptography, blockchain creates a mutually dispersed system that may achieve an agreement without personal intervention. By using cryptography, blockchain creates a mutually dispersed system that may execute a contract without personal intervention. Blockchain is a consensus method that acknowledges the advantages of reaching an agreement between two or more devices without the need of humans. Blockchain applications and cyber-physical systems are transforming traditional business models, technical procedures, and industrial processes. The Bitcoin network's blockchain symbolizes 1.0 technology [4].

An information system innovation is a sophisticated mechanism for administering distributed ledgers to the blockchain [5]. The key features of the traditional notebook system have aroused interest in blockchain technology due to frequent validations of operational transactions for validity, the secrecy of the encoded parties to the transaction, the inaccessibility of the control center, and the establishment of money. Cryptocurrencies are the well-known real-world solution to this new technology. It has about 2000 variations

TABLE 2: Articles selection and final database development process.

Online databases	Papers selected based on title	Papers selected based on abstract	Papers selected based on content provided
IEEE Xplore	252	96	35
ScienceDirect	244	127	39
Hindawi	231	96	27
Springer Link	211	66	25
Total			126

of various modifications. The ever-increasing revenue from cryptocurrencies, especially in the heavily regulated crypto industry, has taken control of exchanges and even specialized bank services as a new asset [6]. Machine vision remains a difficult issue that draws scholars to conduct research in this area. Machine vision systems (MVS) that are inspired by human vision systems have been developed (HVS) [7].

Artificial intelligence (AI) is a broad area of development that can offer a variety of advantages to enterprises. Following an immense quantity of data and a large increase in computing capabilities over the last few years, businesses have increasingly resorted to AI to generate economic value [8]. Global financial services are being reshaped as a result of fast technological advancements and increased competition. AI has recently attracted a lot of attention [9]. Organizations have implemented AI applications to generate more business value in increased sales, revenue, enhanced company efficiency, and cost savings [10]. According to a recent study published in the MIT Sloan Management Review, more than 80% of businesses see AI as a planned opportunity. AI is viewed as a tool to achieve a competitive edge by over 85% of respondents [11]. Various firms invest in AI technology to deal with organizational challenges and revenue development; nevertheless, some businesses fail to see AI's worth [12].

3. Research Protocol

SLR examines and determines a subject of interest by identifying a set of most relevant research questions in the selected research domain. In the SLR process, the research questions serve as a cornerstone. SLR uses a thorough, reliable, and verifiable technique to offer a fair appraisal of a research subject [21]. Many academics in diverse domains like healthcare systems [22], networking [23], crowdsourcing [24], and many others use SLR work to explore the extant and identify the gaps in the literature and define new research direction for the researchers to explore. This SLR method summarizes the literature on artificial intelligence and machine learning approaches used in financial institutions. Following are the list of the objectives that are aimed to be achieved by this systematic research work.

Analyze the current research activity in light of the four research topics that have been defined. These questions aim to outline the existing based on AI models developed to ensure high security in organizations, different types of

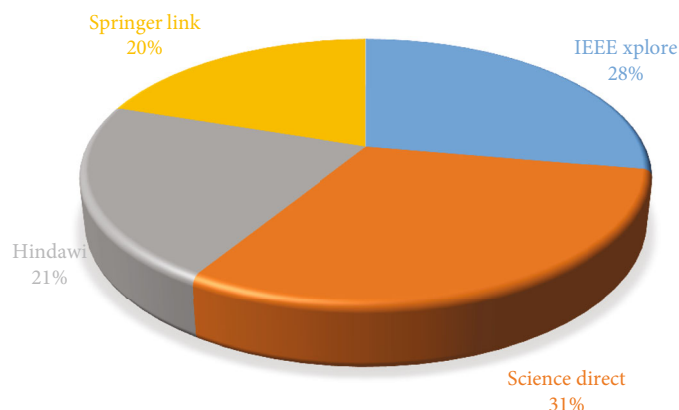


FIGURE 2: Online libraries for the proposed research.

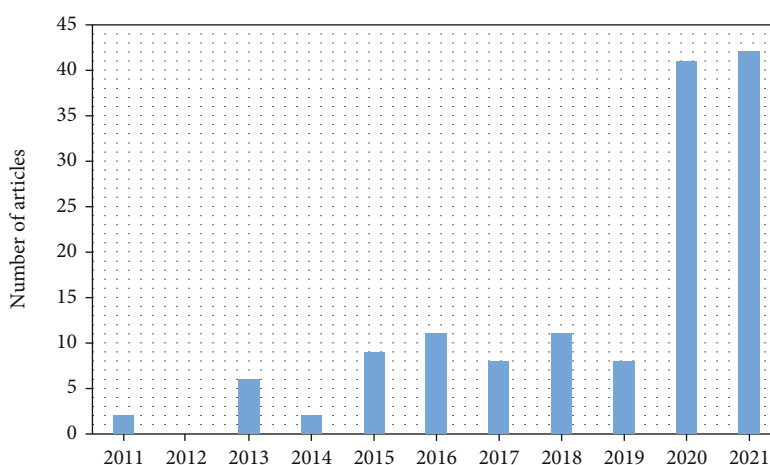


FIGURE 3: Year-wise detail of selected papers.

threats that employees in organizations commonly face, different architectures and tools suggested for mitigating the security risks faced during unwanted situations, and different implications of AI on diverse domains within the organization.

This SLR project attempts to identify significant flaws in existing solutions and propose new future research areas to fill up the gaps. These new study paths will eventually aid firms and staff in assuring high authenticity for their security ways, preventing data leaking, and combating intruder attacks.

The most relevant research publications were chosen from four peer-reviewed internet sources for this SLR project. The researchers will be able to discover the most relevant research publications in the AI area and analyses them using this list of the most relevant research articles.

This SLR paper is being carried out following the guidelines defined by Mishra and Yadav and Daya [26, 27]. The review protocol of this SLR has depicted in Figure 1. It consists of seven main steps: (1) selection of research q, (2) identification of research question, (3) search strategy, (4) selection appropriate studies, (5) review online libraries for most relevant papers selection, (6) quality assessment, and (7) conclusion and future direction. All these stages are described with full description in Figure 1.

3.1. Research Question. Research questions (RQ) are just like the corner stone of any SLR work. The most relevant and highly precised RQs (by considering different aspects in a certain topic of interest) ensure the validity and applicability of the SLR work. To conduct this SLR work, we formulated a set of four RQs to explore the proposed field from different aspects. The details regarding the research questions and the underlined descriptions are detailed below in Table 1.

3.2. Keyword Finalization. After formulating the research questions, the new activity is to identify the most suitable keywords that resultantly helped in accumulating relevant articles from the selected online repositories. The finalized most relevant articles retrieved are “SECURITY, SAFETY, RISKS, THREATS, MITIGATE, MINIMIZE, EMBEDDED, DEPLY, EVIDENCE, PROOF, CAPABILITY, ABILITY, ORGANIZATION, SECTOR, INSTITUTE, IMPACT, OR EFFECT.” These keywords are used for the query development according to the database requirements and tuned further for best outcomes (for the retrieval of satisfactory results in terms of relevant articles).

3.3. Query Selection. To accelerate the articles accumulation process from the selected peer-reviewed libraries, the query

TABLE 3: List of security threats reported in the literature.

S. no	Type of security threat	Description	References
1.	Cyber security	<p>Cyber security has become a topic of worldwide concern and relevance. More than 50 countries have already released a policy statement defining their official positions on cyberspace, cybercrime, and cyber security. Participants with a prior understanding of cyber security could differentiate between distinct cyber-attacks; however, beginner participants were not sensitive to the assault types. For security analysis in corporate networks, it is critical to capture the unpredictable parts of cyber security. However, there has been little research into whether modelling techniques accurately capture such uncertainty, as well as how to design models that are effective in reality. An attack graph depicts the logical causation relationships across numerous privileges and configuration settings in an enterprise network, illustrating probable multistage assaults. Traditional methodologies and technologies to collect, parse, normalize, search, analyze, display, and explore the massive amount of security events gathered by security information and management systems are increasingly reaching their physical limits in many businesses (SIEM). Traditional SIEM devices are meant to statically correlate security events and provide warnings for possible cyber threats in any security operations center (SOC). Every day, billions of security events are generated by a typical company network with thousands of IT systems. The risk management process aids executive decision-making, helping managers and owners to fulfill their fiduciary duty of safeguarding their companies' assets. This critical procedure should not take a long time to complete. The strategy used by an organization to ensure the confidentiality, availability, integrity, nonrepudiation, accountability, authenticity, and dependability of its IT systems is known as information security. The potential use of artificial intelligence technology to ensure data protection. The benefits of utilizing machine learning to analyze data security incidents are demonstrated. A look at some of the most popular commercial information security tools today. The objective of AI applications is to solve problems that take an expert a long time to solve in a short amount of time. The generated model is capable of performing the needed activities in the same manner as an expert advisor. Furthermore, the built software may be utilized by virtually anyone, even if an expert is not present in the business</p>	[15–20, 28–34]
2.	Information security risk (ISR)	<p>The security risks associated with each cloud delivery model differ and are based on a variety of factors, including the sensitivity of information assets, cloud topologies, and security measures implemented in a specific cloud environment. For a better knowledge of essential areas of emphasis in the cloud computing environment, as well as detecting threats and vulnerabilities, use this information risk management approach. Selecting a technique for conducting an information security risk analysis can be difficult for businesses. There are a variety of risk analysis approaches accessible today, some of which are qualitative and others of which are quantitative. The purpose of all of these approaches is to calculate the total risk value. Based on its unique requirements, an organization must choose the best technique. The main goal of information security is to protect an organization's important resources, such as hardware, software, and financial resources, as well as tangible and intangible assets. An organization's security objectives can be addressed by using appropriate security procedures and policies. Artificial intelligence technology excels at supervising and managing tasks in which humans fall short, hence, its use in networking has increased performance and security.</p>	[5, 17, 21–23, 35–38]
3.	Network security	<p>A network risk assessment evaluates the network(s) that your company and workers utilize on a daily basis. Using risk assessment tools, the evaluation helps identify the threats to your essential systems and sensitive data. Cyber-attacks are growing more complicated, and reliable intrusion detection is becoming more difficult (ID). Failure to prevent infiltration can compromise security services such as data integrity, privacy, and availability. The fast growth of computer networks (CNs) has changed how people think about network security. Intrusion detection systems (IDS) are used to detect all types of computer activity and hostile network (NW) traffic that standard firewalls cannot detect. Personal computer users, businesses, and the military have all become more concerned about network security. With the introduction of the internet, security has become a big concern, and studying the history of security helps for a better understanding of how security technologies emerged. Many security issues were possible due to the internet's structure. Firewalls and encryption methods are used by many enterprises to protect themselves from the internet. Businesses construct an "intranet" to stay connected to the internet while protecting themselves from potential risks.</p>	[24, 26, 27, 33]
4.	Security and safety	<p>The attribute or state of being safe, such as being devoid of danger, employment stability, freedom from dread or anxiety, freedom from the risk of being laid off. With changes made both worldwide and nationally, technological breakthroughs improve the way we live. These</p>	[17, 39–43]

TABLE 3: Continued.

S. no	Type of security threat	Description	References
		technological advancements also have unintended consequences in the form of security risks. The use of artificial intelligence (AI) allows to solve complicated problems in the same way that people do. The artificial intelligence (AI) technology detects several assaults that threaten the application and system security of a company. The state of being safe the absence of the possibility of damage, danger, or loss. The ability to avoid or minimize damage, risk, or loss. A contraption or mechanism used to avoid harm or risk. Risk, safety, and security are all ideas that have attracted a lot of scholarly attention. There are a number of assumptions concerning their nature and relationship that have been made. Risk, safety, and security are often used in everyday discourse, in addition to academic contexts.	

TABLE 4: List techniques suggested mitigating security risks.

S. no	Techniques for mitigating security risk	Description	References
1.	Predictive models	Aviation accident investigators have found runway excursion as a significant contributing element in airline landing accidents caused by pilots maintaining an unsafe approach to landing. The goal of this study was to use machine learning to construct and evaluate prediction models for unstable approach risk misperception (UARM) in the National Airspace System	[44]
2.	ISSRM	Organizations' information system security risk management (ISSRM) is critical to their success. ISSRM ensures the availability, integrity, and privacy of information. However, especially in today's enterprises, where activities are done in a complex and interrelated setting, this latter remains a tough region to build and sustain. A well-defined strategy to produce business value is accomplished when an organization's business services and strategic planning are matched with proactive ISSRM operations. To do so, we'll look at risk management methodologies and security modelling languages to see why EAM may be beneficial. The relevance of business intelligence tools as an integrated solution for the insurance industry is growing due to the expanding data sizes in today's business sectors, as well as the requirement of risk management. The majority of the time, these tools have been employed to produce successful risk management.	[45, 46]
3.	Adaptive learning systems	Each discipline is meant to be designed as a workflow for a certain application area made of modules reflecting the necessary areas of knowledge, based on the ideas of "knowledge areas" and "application areas." Through so-called adaptive learning systems, it is possible to significantly improve education by introducing dynamic principles and customization in the curriculum. Furthermore, the management of adaptation may be accomplished using artificial intelligence technologies, which the authors have expertise with in the field of cybersecurity.	[18]
4.	Firewall technology	People's demands for network information technology are growing in tandem with the rapid advancement of science and technology. Artificial intelligence has arisen and is being used in a variety of industries to suit people's unique demands. The goal of incorporating artificial intelligence with computer network technology is to maximize the benefits of both technologies. In this way, computer networks may be utilized to make people's lives and work easier, and AI's function can be customized and humanized. It can also help to preserve information security and improve network administration at the same time. When compared to other defensive technology systems, the intelligent firewall system's combination of AI with firewall provides a greater level of intelligence and information processing impact.	[47]

is formulated ("SECURITY" OR "SAFETY" OR "RISKS" OR "THREATS") AND ("MITIGATE" OR "MINIMIZE") AND ("EMBEDDED" OR "DEPLY") AND ("EVIDENCE" OR "PROOF" OR "CAPABILITY" OR "ABILITY") AND ("SECTOR" OR "ORGANIZATION" OR "INSTITUTE" OR "IMPACT" OR "EFFECT"). This query is fine-tuned depending on the gathered results and the libraries that have been chosen. The 126 most relevant research papers are picked

based on the title, abstract, and content of the research piece. The next paragraph contains a detailed summary of the compiled research publications.

3.4. Review Online Libraries and Final Article Database Development. We selected four of the most peer-reviewed online repositories to accumulate the most relevant research articles for the proposed SLR work, including Hindawi,

TABLE 5: Social and economical impacts of artificial intelligence.

S. no	Types of impacts	Description	References
1.	Fraud detection	<p>Because the mobile channel may accommodate practically any sort of payment, financial theft in the IoT ecosystem is a rapidly expanding concern. Financial fraud in mobile payments has emerged and is becoming more widespread as a result of the fast development of mobile commerce and the IoT environment. Financial fraud causes financial loss in the real world; hence, a highly precise approach of financial fraud detection in an IoT context is required. Furthermore, our technique suggested a machine-learning-based overall procedure for identifying financial fraud and compared it to artificial neural networks for detecting fraud and processing vast volumes of financial data.</p>	[59, 60]
2.	New product innovation	<p>Product lifecycle management (PLM) encompasses a wide range of technical, business, and management operations that occur throughout the lifespan of a product, from the conception of an intangible notion through the recycling of a finished product. AI theories, algorithms, and technologies to distinct stages of PLM (i.e., product design, production, and service) in the context of smart manufacturing.</p>	[61]
3.	Financial prediction models	<p>Despite the rapid development of information science and technology, as well as computer networks, in the last decade, interdisciplinary research that promotes cross-fertilization of disciplines, and the application of research methods used in many other disciplines to financial market forecasting, it remains extremely difficult to predict the current and future state of financial markets. Due to the support of current financial market theories, as well as the relationship between global financial markets and the particular of the forecasting time horizon, financial market forecasting is a difficult study issue.</p>	[62]
4.	Internet supply chain finance	<p>Enterprise green operation is a commercial activity that incorporates environmental preservation into the whole operation and management process of a company. It necessitates that environmental preservation be the driving principle of corporate operations and that every link of business management be founded on it. Furthermore, with the liberalization of the financial sector, banks are no longer the exclusive source of supply chain finance in the nation, owing to the enormous financing demands of SMEs. The use of the internet and big data technologies to address the problem of information symmetry in small and medium-sized firms, as well as to break the chicken-neck of small and medium-sized business finance.</p>	[63]
5.	Interbank offered rate	<p>The interest rate at which banks lend money to one another in the money market is known as the interbank offer rate. Shibor can correctly and timely represent the capital supply and demand connection in the money market as a market-oriented core interest rate, and its changes will immediately transmit and impact China's financial sector. Research is to forecast and investigate the volatility and trend of interbank offer rates, which are the rates at which banks lend money to one another in the money market.</p>	[64]
6.	Financial performance evaluation	<p>In today's competitive market, both businesses and academic institutions place a premium on financial performance evaluation studies. The quality of financial performance has a direct impact on the long-term viability of businesses. Enterprises are paying greater attention to the use of financial performance assessment analysis to promote the sound growth of the entire company as the enterprise management concept deepens. The study-related variables effecting company financial performance, debt-paying capacity, and relevant indicators are chosen from the four aspects of profitability, operation ability, and development ability to design the financial performance assessment system.</p>	[65, 66]
7.	E-commerce	<p>Network flaws in the existing e-commerce operating paradigm, such as network chaos and unequal network distribution, impede economic growth and advancement. Through independent screening and an artificial intelligence system improves and analyses the assembly of e-commerce websites and merges the internet economics with online website theory.</p>	[4]
8.	New product innovation	<p>Currently, there is a growing tendency in enterprises to look at artificial intelligence and nonartificial intelligence for new product innovation and success. The goal of the continuing research is to look into the function of artificial and nonartificial intelligence in new product success, as well as the moderating effect of new product innovation in Chinese manufacturing companies. The findings revealed that both artificial and nonartificial intelligence had a favourable and substantial relationship with new product success.</p>	[61]
9.	Accounting	<p>The continued growth of AI has provided humanity with a plethora of new and unique experiences, as well as a variety of potential future services. Artificial intelligence is an unavoidable scientific and technical outcome of human civilization, as well as a future trend in human growth. In human civilization, accounting is an important financial analytical</p>	[67]

TABLE 5: Continued.

S. no	Types of impacts	Description	References
10.	Financial management	<p>work. Accounting's intelligentization is a microcosm of societal progress. Artificial intelligence can be used to improve financial accounting and support societal development with quicker and smarter services.</p> <p>The linked contents of AI and big data, extensively examines the growth of the financial industry, and demonstrates the application of AI and big data in the area of finance and big data. In the context of big data, a risk evaluation approach for financial information management systems. This approach creates logical nodes based on the system module and then creates a risk estimate model by looking for logical relationships between data.</p>	[68]
11.	Financial crisis	<p>Artificial intelligence is a technological advancement that involves the use of computer systems to do tasks that would normally need human intelligence. This was credited to artificial intelligence management's capacity, as a computer technology, to create, process, and analyze vast amounts of data at once, as opposed to when people are utilized, to assist managers in making speedy decisions because the analysis findings are accessible in real time. According to the study, financial management has a critical role in reducing risks, financial crises, and improving financial performance efficiency in a company or organization.</p>	[69, 70]
12.	Banking	<p>For operational and marketing factors, the present banking business is strongly reliant on technical artifacts backed by intelligent systems. However, the characteristics that enable practice between such technical interfaces and management acceptance have lagged, resulting in a knowledge gap. The paper discusses the influence of AI in financial innovation and the information safety management system (ISMS) in bank financial innovation in the span of AI. Big data, cloud computing, and other technologies have become extensively employed in business and life as a result of the continual development of numerous new internet technologies. The advancement of artificial intelligence technologies has been aided by the expansion of data size and processing capabilities.</p>	[6, 34, 38, 48, 70-74]
13.	Financial sector	<p>A macro view is desperately needed to examine the general nature of AI implementations and how enforcement should be handled within the new frontier of AI technology. The main parameters of the service robotics market include growth rates, volumes, and the scope of service robots, key players are identified. Researchers want to introduce the service of robots to the financial sector.</p>	[6, 75-78]
14.	Governance framework	<p>Because of the widespread use of robots and artificial intelligence (AI) in a variety of industries, including autodrivng, healthcare, military, mass media, service sector, large sets of information searching (legal records), financial services, and new business models, both developed and emerging market economies place a high value on AI development. The revealed scientific governance-based system will be constructed under the premise of responsible research innovation, with the researcher's objective being to establish a governance framework for AI.</p>	[79, 80]
15.	Internal audit	<p>Artificial intelligence (AI) is a technology discipline that stands out for what it can do and the benefits it can bring to a variety of industries. Internal auditing might benefit from incorporating AI into its activities, namely, through the automation of audit procedures that make them faster and more efficient, allowing internal auditors to take on more complicated jobs. Financial fraud and economic losses have paved the way for the development of trustworthy financial big data audit methods. It will assist internal auditors in deducing frauds in a systematic manner while also improving their skills. Internal auditors must adapt to AI's new innovation in order to help firms without losing sight of their goals.</p>	[48, 81, 82]
16.	Education sector	<p>Some study subjects appear to have lasted the test of time as sophisticated technologies in education grow over time, while others have seen peaks and troughs. The goal of the study is to create an international standard-based cyber security system for university education. Each doctrine is recommended to be constructed as a workflow for a certain application area, consisting of modules reflecting the necessary fields of knowledge, based on the ideology of knowing areas and application areas. Through so-called adaptive learning systems, it is possible to significantly improve education by introducing dynamic principles and customization in the curriculum. Furthermore, the management of adaptation may be accomplished using artificial intelligence technologies, which the authors have expertise with in the field of cybersecurity.</p>	[18, 83]
17.	Financial services	<p>The current and potential consequences of artificial intelligence- (AI-) based applications, as well as technical difficulties linked to behavioral finance, are the subject of this research.</p>	[2, 76, 84]

TABLE 5: Continued.

S. no	Types of impacts	Description	References
18.	Validation for quality of service	<p>However, the financial services industry has seen tremendous progress in the field of AI-based applications, particularly in behavioral finance.</p> <p>Based on the input data, a genetic programming-based model is recommended to assure improved customer satisfaction with services. Customers are frequently exploited and subjected to other disruptions in conventional banking and other financial institutions. To address this issue, the authors have presented an effective method for providing and ensuring high-quality services</p>	[85]
19.	Business	<p>Artificial intelligence (AI) is a broad category of technologies that may provide enterprises with a variety of benefits in terms of increased economic value. Following a deluge of data and a significant growth in computing capability, companies have increasingly turned to AI to create commercial value during the last several years. Business process optimization based on artificial intelligence (AI) has a substantial influence on a country's economic progress. We contend that the deployment of artificial neural networks in business processes will aid in optimizing these processes and guaranteeing the appropriate degree of functionality and compliance with the foundations of sustainable development.</p>	[8, 86]
20.	Antimoney laundering	<p>The state-of-the-art AI methodologies for AML, and then propose a framework for next-generation AML solutions that incorporates advanced natural language processing and deep-learning algorithms. Our methodology uses unstructured external data to help domain specialists, with the goal of reducing the human investigator's burden. The study demonstrates the disparity between traditional AML approaches and cutting-edge AI. It emphasizes fresh AI directions that can aid in the development of the AML pipeline, as well as an accessible solution with a lower false positive rate and greater flexibility.</p>	[87, 88]
21.	Product life cycle	<p>Artificial intelligence (AI) technology has recently received a lot of interest in the industrial industry. It attracts a lot of attention as a crucial technology in smart manufacturing and the industry 4.0 agenda. Product lifecycle management (PLM) encompasses a wide range of technical, business, and management operations that occur throughout the lifespan of a product, from the conception of an intangible notion through the disposal of a completed product.</p>	[89]
22.	Investment in firm	<p>Artificial intelligence (AI) has lately acquired traction and attention, resulting in a surge in interest and investment in the field. In comparison to other businesses, nonmanufacturing enterprises and firms with limited information technology skills or low credit ratings incur a more unfavourable impact. The data imply that the majority of investors consider AI investment announcements to be unpleasant news. Following that, the characteristics influencing shareholders' reactions to AI adoption are discussed.</p>	[90]
23.	Business forecasting	<p>The methods and tactics used to forecast company trends such as sales, expenditures, and profits are referred to as business forecasting. The goal of business forecasting is to make better strategies based on these accurate forecasts. Many firms believe that gathering knowledge about the future is critical to ensuring future organizational performance. Managers may make better judgments through improving forecasting progression. A recommendation system including graphical services, database function, reporting, interface, mathematics, and cosmological constants was created for connection recognition.</p>	[91]
24.	Corporate governance	<p>Corporate governance (CG) is important in a company's commitment to and adoption of ethical standards across the board, as well as in interactions with workers, customers, creditors, shareholders, and regulators. The influence of artificial intelligence's continual advancement and adaption on corporate governance. It evaluates the appropriateness, practicality, and responsibility of automating board-level decision-making to guarantee successful corporate governance using three lenses—the business, technology, and society lenses. AI can assist in freeing up government labour by automating repetitive operations, resulting in faster transactions in the delivery of government services and more correctly analyzing the effects of policy alternatives.</p>	[60, 66, 77, 92–94]
25.	Marketing	<p>A growing body of research on intelligent systems/artificial intelligence (AI) in marketing has revealed that AI can imitate people and perform tasks in an 'intelligent' manner. The paradigm provides systematic guidelines for how human marketers and consumers might collaborate with AI in marketing, which has substantial consequences for retailing, which serves as the interface between marketers and customers. For informed consumption decisions, marketers should optimize the mix and timing of AI-HI marketing teams, consumers should comprehend the complementarity between AI and HI capabilities, and</p>	[95, 96]

TABLE 5: Continued.

S. no	Types of impacts	Description	References
		researchers can examine creative methods to and boundary conditions of collaborative intelligence.	
26.	Financial statement	Identifies the danger of severe financial irregularities occurring in the firm based on the yearly financial accounts. These anomalies might be related to many sorts of fraud that do not always influence the yearly financial accounts. The fact that anomalies are large-scale and will have a significant influence on the company's reputation is a distinguishing attribute of them.	[97]
27.	Commercial bank	In both business and society, artificial intelligence (AI) is gaining traction. The earliest uses of AI in banking were effective; nevertheless, AI is mostly used in investment banking and backend services that do not interact with customers. Using an AI-based system in commercial banks to decrease loan losses, enhance payment processing security, organize compliance-related labour, and boost customer happiness.	[88, 98]
28.	Supply chain	Quality client experiences, cost control, and a company's agility in the face of market possibilities and uncertainties are all dependent on supply chains. Companies desire speed, dependability, and traceability while keeping in mind budgetary constraints, deadlines, and inventory management. Supply chains today are substantially different from those of only a few years ago, and they are still evolving in a highly competitive environment. Technology that can cope with the rising complexity of dynamic supply chain operations is required.	[99]
29.	Data governance	Big data algorithmic systems (BDAS), which are frequently based on machine learning, neural networks, and other kinds of artificial intelligence, are made possible by the advent of big, open, and linked data (BOLD) (AI). When a result, as systems are increasingly asked to make decisions that affect individuals, communities, and society as a whole, failures cannot be allowed, and they must adhere to strict legal and ethical criteria. They all, however, rely on data that is not just large, open, and interconnected, but also diverse, dynamic, and transmitted at high rates in real time.	[100]
30.	Business and economics	The industrial age, which mankind began long ago with the invention of steam power, resulted in rudimentary automation in manufacturing. Electronics, nanotechnology, breakthroughs in medicine, health, and digital applications, among other things, have all accelerated mechatronics research in recent years. The study demonstrates that altering the way businesses are conducted via the use of innovative technologies will have new effects on day-to-day operations as well as the export of these nations' economies to the global economy. As AI and robotics improve, many substances and services related to business and economics will face serious threats, exposures, hits, change, and opportunities, such as performance, jobless ratio, management, customer relationship management, sales, strategic planning, mass production, CRM analytics GDP, purchasing power parity, inflation, money, central banks, banking system, training, accounting, taxes, coaching, and so on	[101]
31.	Cash flow	Cash flow is currently one of the most essential notions in financial analysis. Large commercial banks' financial strategy relies heavily on cash flow forecasting. Forecasting cash flow is an essential aspect of the region's cash flow management process. In the event of a forecasting error, there may be a cash shortage in one of the currencies or an overflow of bank branch vaults, necessitating additional charges for strengthening or exporting money. Many variables impact money movement, including political, economic, and geographical considerations	[102]
32.	Open data	The goal of this study is to assess the adoption of OD technology in Kuwait and to obtain company owners' perspectives on the concept's capacity to be adopted. Our strategy for getting various opinions and points of view concerning this technology was to create an online and hardcopy survey. We aimed to concentrate on the private sector, and we targeted individuals who operate a business and want to provide better services to their clients.	[103]
33.	Earnings equity	The impact of corporate social responsibility disclosure (CSR) on earnings quality (EQ) in Gulf Cooperation Council member nations is investigated in this study (GCC). Corporate social responsibility (CSR), which has gotten a lot of attention in accounting and finance, has piqued the interest of accounting scholars. CSR has always combined social and corporate operations.	[72]
34.	Annual reports	Academics and scholars have been paying close attention to business sustainability and social responsibility in recent years. It has long been recognized that corporate financial performance is linked to, among other things, long-term corporate economic growth. All firms are encouraged to voluntarily report all aspects of their sustainability in order to	[72]

TABLE 5: Continued.

S. no	Types of impacts	Description	References
35.	Firm financing	improve the accountability and transparency of their operations and assist investors in properly valuing them. The majority of equity issuances occur in local markets, whereas bonds and loans are typically issued globally, have long maturities, and have minimal credit risk. In comparison to worldwide norms, the Arab region's issuing corporations are quite substantial. While the sums raised in the stock and credit markets (as a percentage of GDP) are high by international standards, bond issuance activity is low. Bond finance, on the other hand, has grown in importance over time.	[73, 104]
36.	Stock market	The stock markets in the Middle East are expanding at a breakneck speed. The goal is to identify the stock markets of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates' market dynamics and real-time interactions. While return behavior is certainly not uniform, there is evidence of growing market integration.	[105, 106]
37.	IRFS	Recent advancements and changes in corporate governance (CG), as well as the ongoing discussion in the international accounting literature over the implementation of IFRS, have revealed a number of major deficiencies that have yet to be addressed. Many issues concerning the role of CG in the implementation of IFRS, particularly in Gulf member nations, remain unaddressed. Almost all prior research on the influence and link between CG and IFRS adoption was conducted in wealthy nations.	[94, 107]
38.	IT governance	Advancements in information and telecommunications technologies, information technology (IT) governance has become increasingly important in enterprises and organizations. IT governance has evolved into a valuable asset for every business, and it is now seen as a key to success and profit generation.	[34]
39.	Human resources management	Artificial intelligence is a true corporate innovation that will have a significant influence on how workers operate, particularly in the human resources and employment departments.	[108]

Springer Link, IEEE Xplore, and ScienceDirect. A total of 126 most relevant research articles are finalized for assessment and evaluation purposes. The description regarding final database development and relevant articles selection is described in Table 2.

A total of 126 research articles are finalized for the assessment and evaluation purposes. The number of articles contributed in this final pool from the selected different peer-reviewed online repositories is depicted in Figure 2.

With the passage of time, artificial intelligence has become a fascinating and appealing area for researchers all around the world. The researchers used artificial intelligence and machine learning techniques extensively in a variety of disciplines, including healthcare, tracking and navigation, internet security, and business and lucrative sectors and organizations. Based on these applications researchers used these models in financial firms to assure strong security and integrity of their personnel. Figure 3 shows the annual contribution of various research publications in the suggested subject depending on the research questions selected.

After evaluating the results shown in Figure 3, it is concluded that with passage of time, the number of research articles exponentially increases that reflects the interest of researchers in the proposed domain. After 2019, the number of publication increased abruptly that shows the interest of the organizations for ensuring high security and safety for its employees and other assets.

4. Quality Assessment

After the development of a final selection of relevant articles, the next critical step is to evaluate all of the relevant articles using the criteria that have been established [13]. For the assessment purposes in this research work, a quality criterion (QC) has defined given below:

- (i) If an article fully satisfies an inevitable selected research question, then that particular paper is assigned a weighted value of 1
- (ii) While if a paper fails to satisfy to answer any particular research question, it was awarded a weighted value of 0

5. Results and Analysis

The findings of this SLR study are summarized in this portion of the publication. The relevant papers, as well as their emphasized descriptions in relation to each study topic, are detailed below.

5.1. What Are the Various Types of Organizational Security Risks Faced by Employees Working within the GCC Region?
This research question has outlined different security threats typically faced within the financial sectors in the GCC region [14]. In this modern technological age, dangers and consequences vary from types of threats and organizations. The prime objective of this research question is to outline

different threats reported in the extant and find out what type of new threats are available, or we face in common. Table 3 represents the list of security threats most reported in the literature.

5.2. By Utilizing AI Capabilities as Evidence, How Many Proactive Approaches Are Proposed to Counter Organizational Security Risks in the GCC Region? This research question has offered a variety of ways for securing systems within an organization by utilizing AI capabilities. The major goal of this research topic is to describe the many proactive techniques to reducing security risk. Table 4 shows a list of several sorts of security risk mitigation techniques that have been recommended for use within businesses.

5.3. Based on the Extant Findings, How Can We Improve the Capabilities of the Available Authentication Systems in the GCC Organizations? Most firms compete not only in their field of competence but also in being the leaders and innovators in the use of new applications and innovative technology. This fast growth in reliance on technology and its usage to process meaningful data has become a key audit problem for any firm [48]. In our current technology age, artificial intelligence and machine learning models have been widely proposed for a variety of research topics spanning from healthcare [49] to navigation systems [50, 51], face recognition to object detection and recognition [52, 53], and many others. The usage of mobile devices with access to vital resources is increasing, which increases the attack surface of digital assets. A smartphone or laptop can now be used to access a private company's network or data. The goal is to identify the many technologies involved in the implementations of continuous authentication, as well as the assessment methodologies and application cases [54]. This study attempts to present the recommended ways in the field of financial organization to ensure high security and authenticity, taking into account the varied applications of AI and machine learning techniques. Researchers throughout the world have presented several ways based on both deep and shallow architectures to assure high security and resist unauthorized access to security systems within businesses, and overall identification and recognition rates are comparably much better.

To tackle the low accuracy rates of multiclass issues while also reducing simulation time, the researchers focused on hybrid models (deep-deep architectures, deep-shallow architectures, and so on), in which one architecture/classifier does one task while the other performs another. This cuts down on simulation time while ensuring excellent recognition rates. Using data fusion-based hybrid deep learning models, such models are presented for face verification [55], and many others. Given the importance of hybrid models, integrating sophisticated hybrid and AI models within financial institutions is the greatest way for providing high security for clients and investors.

5.4. What Are the Social and Economic Impacts of AI on Financial Bodies Operating in the GCC Region? Artificial intelligence has a wide range of effects on our lives and has

a wide range of cutting-edge applications in a variety of fields. It has reduced human labour in numerous research disciplines, such as text recognition, by offering automated applications [56, 57], network security [57], and healthcare domain [51, 58]. Table 5 represents the list of social and economical impacts of the artificial intelligence in different financial organizations.

6. Limitations

This research article has outlined 126 most relevant articles by analyzing the techniques developed to restrict unauthorized access in the organizations. Besides some key advantages, the following are the limitations of this systematic mapping:

- (i) Only four most peer-reviewed research libraries are selected for the articles accumulation and downloading purposes. Though there are a massive number of online repositories exist. Still, our prime concern was to select only those extensively searched and reviewed libraries by most researchers
- (ii) This SLR work is executed only for ten years, but the papers are published daily in artificial intelligence
- (iii) Only published research work is selected for assessment and analysis purposes. No under-review or the work under simulations in the labs is considered for evaluation and analysis purposes
- (iv) The papers are accumulated using keywords and formulated queries. So, if an article has no synonym matching the keywords, that paper was skipped during the article accumulation process. Also, if a paper has only a word relevant to artificial intelligence or machine learning, that paper was also skipped (if it fails to satisfy the selected research question or has no content pertinent to financial organizations)

7. Conclusions

AI has demonstrated exceptional skills in a variety of disciplines, including the financial and regulatory industries. Financial sectors in GCC countries are facing serious issues in terms of security, safety, and fraudulent activities as a result of the rise of information technology and smart apps. These challenges are significant roadblocks to financial companies' success, and in most situations, they result in significant losses in the form of cash loss, information theft, and so on. This work gives a systematic analysis by assessing the most relevant research publications gathered from peer-reviewed online repositories in order to address these challenges and present new future research paths for assuring high security, privacy, and safety. These articles were assessed for (1) recognizing the difficulties facing or faced by financial sector of GCC region most typically, (2) to describe the many strategies offered to address these

difficulties, as well as where these solutions fall short, (3) how artificial intelligence-based solutions have been used to handle these problems and how they may be enhanced to ensure high levels of security and authenticity, and (4) what are the social and economic importance of AI on our lives and other sectors. Based on this systematic analysis, new research directions are proposed to ensure a safe and secure environment within the organizations for both employees and the owners.

8. Implications

This article has a lot of consequences in the financial sector of GCC region. The effectiveness of many processes will be improved by applying artificial intelligence skills in financial industry. Artificial intelligence, hybrid technology, and protocols can be used to safeguard data access for employees and financial institutions. Financial businesses should make data access control a solid policy decision that supports employee honesty, justice, and equality.

Data Availability

All related data is available in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest

Acknowledgments

The Qatar University Internal Grant no. QUHI-CBE-21/22-1 funded this publication.

References

- [1] S. M. C. Loureiro, J. Guerreiro, and I. Tussyadiah, "Artificial intelligence in business: state of the art and future research agenda," *Journal of Business Research*, vol. 129, pp. 911–926, 2021.
- [2] J. Lee, "Access to finance for artificial intelligence regulation in the financial services industry," *European Business Organization Law Review*, vol. 21, no. 4, pp. 731–757, 2020.
- [3] M. Lu, P. Corriveau, L. Koons, and D. Boyer, "Information technology service delivery to small businesses," in *International Conference on HCI in Business*, pp. 60–67, Springer, 2014.
- [4] S. Li, "Structure optimization of e-commerce platform based on artificial intelligence and blockchain technology," *Wireless Communications and Mobile Computing*, vol. 2020, 8 pages, 2020.
- [5] K. AlJemy, M. AlAnazi, M. AlSofiry, and A. Baig, "Improving IoT security using blockchain," in *2019 IEEE 10th GCC Conference & Exhibition (GCC)*, pp. 1–6, Kuwait, Kuwait, 2019.
- [6] I. A. Kruglova and V. A. Dolbezhkin, "Objective barriers to the implementation of blockchain technology in the financial sector," in *2018 International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI)*, pp. 47–50, Nicosia, Cyprus, 2018.
- [7] M. Al-Azawi, Y. Yang, and H. Istance, "Human attention-based regions of interest extraction using computational intelligence," in *2015 IEEE 8th GCC Conference & Exhibition*, pp. 1–6, Muscat, Oman, 2015.
- [8] I. M. Enholm, E. Papagiannidis, P. Mikalef, and J. Krogstie, "Artificial intelligence and business value: a literature review," *Information Systems Frontiers*, pp. 1–26, 2021.
- [9] M. Riikkinen, H. Saarijärvi, P. Sarlin, and I. Lähteenmäki, "Using artificial intelligence to create value in insurance," *International Journal of Bank Marketing*, vol. 36, no. 6, pp. 1145–1168, 2018.
- [10] S. AlSheibani, C. Messom, and Y. Cheung, "Re-thinking the competitive landscape of artificial intelligence," in *Proceedings of the 53rd Hawaii international conference on system sciences*, Hawaii, USA, 2020.
- [11] S. Ransbotham, D. Kiron, P. Gerbert, and M. Reeves, "Reshaping business with artificial intelligence: closing the gap between ambition and action," *MIT Sloan Management Review*, vol. 59, 2017.
- [12] T. Fountaine, B. McCarthy, and T. Saleh, "Building the AI-powered organization," *Harvard Business Review*, vol. 97, pp. 62–73, 2019.
- [13] H. U. Khan, M. K. Alomari, S. Khan et al., "Systematic analysis of safety and security risks in smart homes," *CMC-Computers Materials & Continua*, vol. 68, no. 1, pp. 1409–1428, 2021.
- [14] M. Al-Saidi, "Cooperation or competition? State environmental relations and the SDGs agenda in the Gulf Cooperation Council (GCC) region," *Environment and Development*, vol. 37, article 100581, 2021.
- [15] H. M. Farooq and N. M. Otaibi, "Optimal machine learning algorithms for cyber threat detection," in *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*, pp. 32–37, Cambridge, UK, 2018.
- [16] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial intelligence in cyber threats intelligence," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pp. 1–4, Mon Tresor, Mauritius, 2018.
- [17] J. Link, K. Waedt, I. B. Zid, and X. Lou, "Current challenges of the joint consideration of functional safety & cyber security, their interoperability and impact on organizations: how to manage RAMS+ S (reliability availability maintainability safety+ security)," in *2018 12th International Conference on Reliability, Maintainability, and Safety (ICRMS)*, pp. 185–191, Shanghai, China, 2018.
- [18] R. Trifonov, O. Nakov, S. Manolov, G. Tsochev, and G. Pavlova, "Possibilities for improving the quality of cyber security education through application of artificial intelligence methods," in *2020 International Conference Automatics and Informatics (ICAI)*, pp. 1–4, Varna, Bulgaria, 2020.
- [19] B. Thuraisingham, "The role of artificial intelligence and cyber security for social media," in *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, pp. 1–3, New Orleans, LA, USA, 2020.
- [20] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Computer Science*, vol. 2, no. 3, pp. 1–18, 2021.
- [21] M. Dhingra, M. Jain, and R. S. Jadon, "Role of artificial intelligence in enterprise information security: a review," in *2016 fourth international conference on parallel, distributed and grid computing (PDGC)*, pp. 188–191, Wanknaghat, India, 2016.

- [22] Y. Xiao-yang, "Study on development of information security and artificial intelligence," in *2011 Fourth International Conference on Intelligent Computation Technology and Automation*, pp. 248–250, Shenzhen, China, 2011.
- [23] N. Mavridis, G. Pierris, C. BenAbdelkader, A. Krstikj, and C. Karaiskos, "Smart buildings and the human-machine cloud," in *2015 IEEE 8th GCC Conference & Exhibition*, pp. 1–6, Muscat, Oman, 2015.
- [24] Y. Zhen, A. Khan, S. Nazir, Z. Huiqi, A. Alharbi, and S. Khan, "Crowdsourcing usage, task assignment methods, and crowdsourcing platforms: a systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 8, article e2368, 2021.
- [25] B. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep. EBSE-2007-01, 2007, Softw. Eng. Group School Comput. Sci. Math. Keele Univ., Keele, U.K. and Dept. of Comput. Sci. Univ. Durham, Durham, U.K, 2007.
- [26] A. Mishra and P. Yadav, "Anomaly-based IDS to detect attack using various artificial intelligence & machine learning algorithms: a review," in *2nd International Conference on Data, Engineering and Applications (IDEA)*, pp. 1–7, Bhopal, India, 2020.
- [27] B. Daya, *Network Security: History, Importance, and Future*, vol. 4, University of Florida Department of Electrical and Computer Engineering, 2013.
- [28] J. H. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018.
- [29] B. Alhayani, H. J. Mohammed, I. Z. Chalooob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," *Materials Today: Proceedings*, 2021.
- [30] B. D. Deebak and A.-T. Fadi, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements," *Journal of Information Security and Applications*, vol. 58, article 102749, 2021.
- [31] Y. Peng and Q. Wu, "Secure communication and access control for web services container," in *2006 Fifth International Conference on Grid and Cooperative Computing (GCC'06)*, pp. 412–415, Hunan, China, 2006.
- [32] A. K. Alharam and W. Elmedany, "The effects of cyber-security on healthcare industry," in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, pp. 1–9, Manama, Bahrain, 2017.
- [33] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using Bayesian networks for cyber security analysis," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, pp. 211–220, Chicago, IL, 2010.
- [34] Y. Alansari and A. M. A. Musleh Al-Sartawi, "IT governance and E-banking in GCC listed banks," *Procedia Computer Science*, vol. 183, pp. 844–848, 2021.
- [35] H. Sato, "A new formula of security risk analysis that takes risk improvement factor into account," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, pp. 1243–1248, Boston, MA, USA, 2011.
- [36] S. Erokhin, "Artificial intelligence for information security," in *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1–4, Moscow, Russia, 2020.
- [37] Y. A. Basallo, V. E. Senti, and N. M. Sanchez, "Artificial intelligence techniques for information security risk assessment," *IEEE Latin America Transactions*, vol. 16, no. 3, pp. 897–901, 2018.
- [38] X. Hu and K. Wang, "Bank financial innovation and computer information security management based on artificial intelligence," in *2020 2nd international conference on machine learning, Big Data and Business Intelligence (MLBDBI)*, pp. 572–575, Taiyuan, China, 2020.
- [39] A. Guzman, S. Ishida, E. Choi, and A. Aoyama, "Artificial intelligence improving safety and risk analysis: a comparative analysis for critical infrastructure," in *2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 471–475, Bali, Indonesia, 2016.
- [40] U. Kose and P. Vasant, "Fading intelligence theory: a theory on keeping artificial intelligence safety for the future," in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 1–5, Malatya, Turkey, 2017.
- [41] S. Srivastava, A. Bisht, and N. Narayan, "Safety and security in smart cities using artificial intelligence—a review," in *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 130–133, Noida, India, 2017.
- [42] K. Rindell and J. Holvitie, "Security risk assessment and management as technical debt," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–8, Oxford, UK, 2019.
- [43] D. Dai and S. Boroomand, "A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges," *Archives of Computational Methods in Engineering*, vol. 29, no. 2, pp. 1291–1309, 2022.
- [44] E. V. Odisho and D. Truong, "Applying machine learning to enhance runway safety through runway excursion risk mitigation," in *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, pp. 1–10, Dulles, VA, USA, 2021.
- [45] W. Abbass, A. Baina, and M. Bellafkih, "Improvement of information system security risk management," in *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 182–187, Tangier, Morocco, 2016.
- [46] M. Amini, S. Salimi, F. Yousefnejad, M. J. Tarokh, and S. M. Haybatollahi, "The implication of business intelligence in risk management: a case study in agricultural insurance," *Journal of Data, Information and Management*, vol. 3, no. 2, pp. 155–166, 2021.
- [47] X. Shang and C. Zhao, "Research on the application of artificial intelligence in computer network technology," in *2020 5th international conference on mechanical, Control and Computer Engineering (ICMCCE)*, pp. 1107–1110, Harbin, China, 2020.
- [48] A. A. Lawati and S. Ali, "Business perception to learn the art of operating system auditing: a case of a local bank of Oman," in *2015 IEEE 8th GCC Conference & Exhibition*, pp. 1–6, Muscat, Oman, 2015.
- [49] R. Alshamsan, H. Leslie, A. Majeed, and M. Kruk, "Financial hardship on the path to universal health coverage in the Gulf states," *Health Policy*, vol. 121, no. 3, pp. 315–320, 2017.
- [50] K. Zhu and T. Zhang, "Deep reinforcement learning based mobile robot navigation: a review," *Tsinghua Science and Technology*, vol. 26, no. 5, pp. 674–691, 2021.

- [51] S. P. Singh, L. Wang, S. Gupta, B. Gulyas, and P. Padmanabhan, "Shallow 3D CNN for detecting acute brain hemorrhage from medical imaging sensors," *IEEE Sensors Journal*, vol. 21, no. 13, pp. 14290–14299, 2021.
- [52] W. AbdAlmageed, Y. Wu, S. Rawls et al., "Face recognition using deep multi-pose representations," in *2016 IEEE winter conference on applications of computer vision (WACV)*, pp. 1–9, Lake Placid, NY, USA, 2016.
- [53] M. Yasir, M. S. Hossain, S. Nazir, S. Khan, and R. Thapa, "Object identification using manipulated edge detection techniques," *Science*, vol. 3, no. 1, pp. 1–6, 2022.
- [54] J. Junquera-Sánchez, C. Cilleruelo, L. De-Marcos, and J.-J. Martínez-Herráiz, "Access control beyond authentication," *Security and Communication Networks*, vol. 2021, 11 pages, 2021.
- [55] Y. Sun, X. Wang, and X. Tang, "Hybrid deep learning for face verification," in *Proceedings of the IEEE international conference on computer vision*, pp. 1489–1496, Sydney, NSW, Australia, 2013.
- [56] D. Coquenot, C. Chatelain, and T. Paquet, "End-to-end handwritten paragraph text recognition using a vertical attention network," *Institute of Electrical and Electronics Engineers transactions on pattern analysis and machine intelligence*, p. 1, 2022.
- [57] J. H. Lee, T. Ernst, and N. Chilamkurti, "Performance analysis of PMIPv6-based network mobility for intelligent transportation systems," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 74–85, 2012.
- [58] H. Chen, S. Khan, B. Kou, S. Nazir, W. Liu, and A. Hussain, "A smart machine learning model for the detection of brain hemorrhage diagnosis based internet of things in smart cities," *Complexity*, vol. 2020, Article ID 3047869, 2020.
- [59] D. Choi and K. Lee, "An artificial intelligence approach to financial fraud detection under IoT environment: a survey and implementation," *Security and Communication Networks*, vol. 2018, Article ID 5483472, 2018.
- [60] H.-A. N. Al-Malkawi, R. Pillai, and M. I. Bhatti, "Corporate governance practices in emerging markets: the case of GCC countries," *Economic Modelling*, vol. 38, pp. 133–141, 2014.
- [61] H. Jianjun, Y. Yao, J. Hameed et al., "The role of artificial and nonartificial intelligence in the new product success with moderating role of new product innovation: a case of manufacturing companies in China," *Complexity*, vol. 2021, Article ID 8891298, 2021.
- [62] H. Jia, "Deep learning algorithm-based financial prediction models," *Complexity*, vol. 2021, Article ID 5560886, 2021.
- [63] J. Zhang, "Development of internet supply chain finance based on artificial intelligence under the enterprise green business model," *Mathematical Problems in Engineering*, vol. 2021, Article ID 9947811, 2021.
- [64] W. Xie, "Interbank offered rate based on artificial intelligence algorithm," *Mathematical Problems in Engineering*, vol. 2021, Article ID 9931539, 2021.
- [65] Z. Chen, "Research on accounting intelligence system modeling of financial performance evaluation," *Security and Communication Networks*, vol. 2021, Article ID 5550382, 2021.
- [66] W. M. Al-ahdal, M. H. Alsamhi, M. I. Tabash, and N. H. S. Farhan, "The impact of corporate governance on financial performance of Indian and GCC listed firms: an empirical investigation," *Research in International Business and Finance*, vol. 51, article 101083, 2020.
- [67] Z. Li, "Analysis on the influence of artificial intelligence development on accounting," in *2020 International conference on big data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, pp. 260–262, Fuzhou, China, 2020.
- [68] N. Wang, Y. Liu, Z. Liu, and X. Huang, "Application of artificial intelligence and big data in modern financial management," in *2020 International Conference on Artificial Intelligence and Education (ICAIE)*, pp. 85–87, Tianjin, China, 2020.
- [69] V. K. Shah, "Artificial intelligence management in financial crisis," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICIC)*, pp. 1–6, Madurai, India, 2015.
- [70] F. Alqahtani and D. G. Mayes, "Financial stability of Islamic banking and the global financial crisis: evidence from the Gulf Cooperation Council," *Economic Systems*, vol. 42, no. 2, pp. 346–360, 2018.
- [71] R. Arjun, A. Kuanr, and K. Suprabha, "Developing banking intelligence in emerging markets: systematic review and agenda," *International Journal of Information Management Data Insights*, vol. 1, article 100026, 2021.
- [72] M. K. Al Ani, "Corporate social responsibility disclosure and financial reporting quality: evidence from Gulf Cooperation Council countries," *Borsa Istanbul Review*, vol. 21, pp. S25–S37, 2021.
- [73] R. Al-Khouri and H. Arouri, "The simultaneous estimation of credit growth, valuation, and stability of the Gulf Cooperation Council banking industry," *Economic Systems*, vol. 40, no. 3, pp. 499–518, 2016.
- [74] S. Srairi, "Transparency and bank risk-taking in GCC Islamic banking," *Borsa Istanbul Review*, vol. 19, pp. S64–S74, 2019.
- [75] A. V. Bataev, N. Dedyukhina, and M. N. Nasrutdinov, "Innovations in the financial sphere: performance evaluation of introducing service robots with artificial intelligence," in *2020 9th International Conference on Industrial Technology and Management (ICITM)*, pp. 256–260, Oxford, UK, 2020.
- [76] M. Shanmuganathan, "Behavioural finance in an era of artificial intelligence: longitudinal case study of robo-advisors in investment decisions," *Journal of Behavioral and Experimental Finance*, vol. 27, article 100297, 2020.
- [77] A. A.-N. Abdallah, M. K. Hassan, and P. L. McClelland, "Islamic financial institutions, corporate governance, and corporate risk disclosure in Gulf Cooperation Council countries," *Journal of Multinational Financial Management*, vol. 31, pp. 63–82, 2015.
- [78] A. Maghyreh and H. Abdoh, "The effect of structural oil shocks on bank systemic risk in the GCC countries," *Energy Economics*, vol. 103, article 105568, 2021.
- [79] H. Zhang and L. Gao, "Shaping the governance framework towards the artificial intelligence from the responsible research and innovation," in *2019 IEEE International Conference on Advanced Robotics and its Social Impacts (ARSO)*, pp. 213–218, Beijing, China, 2019.
- [80] P. G. R. de Almeida, C. D. dos Santos, and J. S. Farias, "Artificial intelligence regulation: a framework for governance," *Ethics and Information Technology*, vol. 23, pp. 1–21, 2021.
- [81] B. Couceiro, I. Pedrosa, and A. Marini, "State of the art of artificial intelligence in internal audit context," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–7, Seville, Spain, 2020.

- [82] Z. Zhang and Z. Wang, "Design of financial big data audit model based on artificial neural network," *International Journal of Systems Assurance Engineering and Management*, pp. 1–10, 2021.
- [83] C. Guan, J. Mou, and Z. Jiang, "Artificial intelligence innovation in education: a twenty-year data-driven historical analysis," *International Journal of Innovation Studies*, vol. 4, no. 4, pp. 134–147, 2020.
- [84] J. Y. Huang, A. Gupta, and M. Youn, "Survey of EU ethical guidelines for commercial AI: case studies in financial services," *AI and Ethics*, vol. 1, no. 4, pp. 569–577, 2021.
- [85] M. Castelli, L. Manzoni, and A. Popovič, "An artificial intelligence system to predict quality of service in banking organizations," *Computational Intelligence and Neuroscience*, vol. 2016, Article ID 9139380, 2016.
- [86] K. A. Rashedi, M. T. Ismail, N. N. Hamadneh, S. A. Wadi, J. J. Jaber, and M. Tahir, "Application of radial basis function neural network coupling particle swarm optimization algorithm to classification of Saudi Arabia stock returns," *Journal of Mathematics*, vol. 2021, Article ID 5593705, 2021.
- [87] J. Han, Y. Huang, S. Liu, and K. Towey, "Artificial intelligence for anti-money laundering: a review and extension," *Digital Finance*, vol. 2, no. 3–4, pp. 211–239, 2020.
- [88] M. Turki, A. Hamdan, R. T. Cummings, A. Sarea, M. Karolak, and M. Anasweh, "The regulatory technology "RegTech" and money laundering prevention in Islamic and conventional banking industry," *Heliyon*, vol. 6, no. 10, article e04949, 2020.
- [89] L. Wang, Z. Liu, A. Liu, and F. Tao, "3D printing of aluminum alloys using laser powder deposition: a review," *The International Journal of Advanced Manufacturing Technology*, vol. 116, no. 1–2, pp. 1–37, 2021.
- [90] A. K. Lui, M. C. Lee, and E. W. Ngai, "Impact of artificial intelligence investment on firm value," *Annals of Operations Research*, vol. 308, no. 1–2, pp. 373–388, 2022.
- [91] B. Li, C. Yao, F. Zheng, L. Wang, J. Dai, and Q. Xiang, "Intelligent decision support system for business forecasting using artificial intelligence," *Arabian Journal for Science and Engineering*, pp. 1–11, 2021.
- [92] M. Hilb, "Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance," *Journal of Management and Governance*, vol. 24, no. 4, pp. 851–870, 2020.
- [93] G. D. Sharma, A. Yadav, and R. Chopra, "Artificial intelligence and effective governance: a review, critique and research agenda," *Sustainable Futures*, vol. 2, article 100004, 2020.
- [94] F. A. Almaqtari, A. A. Hashed, and M. Shamim, "Impact of corporate governance mechanism on IFRS adoption: a comparative study of Saudi Arabia, Oman, and the United Arab Emirates," *Heliyon*, vol. 7, no. 1, article e05848, 2021.
- [95] M.-H. Huang and R. T. Rust, "A framework for collaborative artificial intelligence in marketing," *Journal of Retailing*, 2021.
- [96] B. Vlačić, L. Corbo, S. C. e Silva, and M. Dabić, "The evolving role of artificial intelligence in marketing: a review and research agenda," *Journal of Business Research*, vol. 128, pp. 187–203, 2021.
- [97] J. Wyrobek, "Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair corporate culture," *Procedia Computer Science*, vol. 176, pp. 3037–3046, 2020.
- [98] F. Königstorfer and S. Thalmann, "Applications of artificial intelligence in commercial banks - a research agenda for behavioral finance," *Journal of Behavioral and Experimental Finance*, vol. 27, article 100352, 2020.
- [99] Y. Riahi, T. Saikouk, A. Gunasekaran, and I. Badraoui, "Artificial intelligence applications in supply chain: a descriptive bibliometric analysis and future research directions," *Expert Systems with Applications*, vol. 173, article 114702, 2021.
- [100] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: organizing data for trustworthy artificial intelligence," *Government Information Quarterly*, vol. 37, no. 3, article 101493, 2020.
- [101] C. Dirican, "The impacts of robotics, artificial intelligence on business and economics," *Procedia-Social and Behavioral Sciences*, vol. 195, pp. 564–573, 2015.
- [102] K. Dadteev, B. Shchukin, and S. Nemeshaev, "Using artificial intelligence technologies to predict cash flow," *Procedia Computer Science*, vol. 169, pp. 264–268, 2020.
- [103] N. Alawadhi, I. Al Shaikhli, A. Alkandari, and S. K. Chab, "Business owners' feedback toward adoption of open data: a case study in Kuwait," *Journal of Electrical and Computer Engineering*, vol. 2021, Article ID 6692410, 2021.
- [104] J. J. Cortina, S. Ismail, and S. L. Schumker, "Firm financing and growth in the Arab region," *Economic Systems*, vol. 42, no. 2, pp. 361–383, 2018.
- [105] J. Bley and K. H. Chen, "Gulf Cooperation Council (GCC) stock markets: the dawn of a new era," *Global Finance Journal*, vol. 17, no. 1, pp. 75–91, 2006.
- [106] N. T. Hung, "Financial connectedness of GCC emerging stock markets," *Economic Review*, vol. 11, no. 4, pp. 753–773, 2021.
- [107] M. Abdelqader, K. Nimer, and T. K. Darwish, "IFRS compliance in GCC countries: do corporate governance mechanisms make a difference?," *International Journal of Disclosure and Governance*, vol. 18, no. 4, pp. 411–425, 2021.
- [108] M. M. Abdeldayem and S. H. Aldulaimi, "Trends and opportunities of artificial intelligence in human resource management: aspirations for public sector in Bahrain," *International Journal of Scientific and Technology Research*, vol. 9, pp. 3867–3871, 2020.