Journal of Intelligent Decision Making and Information Science

www.jidmis.org.org
eISSN: 3079-0875

PERAM: An Efficient Readiness Assessment Model for the Banking Industry to Implement IoT – A Systematic Review and Fuzzy SWARA Methods

Mahmoud Zahedian Nezhad[1,*], Javad Nazarian-Jashnabadi[2,*], Mohammad Mehraeen[3], Javad Rezazadeh[4]

[1] Faculty of Economic and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad, Iran. Azadi Square, Mashhad, Razavi Khorasan Province, Iran. Phone: +985138802415. Postal Code: 9177948974. *Email:* mahmoud.zahediannezhad@mail.um.ac.ir
[2] Department of Management, Faculty of Economic, Management and Social Science, Shiraz University, Shiraz, Iran. Email: J_Nazarian@shirazu.ac.ir
[3] Faculty of Economic and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad, Iran. Email: m-lagzian@um.ac.ir
[4] Crown Institute of Higher Education (CIHE), Sydney, Australia. Email: javad.rezazadeh@cihe.edu.au

ARTICLE INFO

Article history:
Received 18 November 2024
Received in revised form 20 December 2024
Accepted 25 December 2024
Available online 28 December 2024

Keywords:
Internet of Things; Readiness; Banking; Systematic Review; Fuzzy SWARA; Decision Making

ABSTRACT

Since the emergence of the IoT and its significant benefits, various economic, social, and political groups have been deploying and implementing IoT in different sectors. The large amounts of data generated from connected devices and products can be analysed, transforming the goals and attitudes of businesses and industries, including the banking industry. However, implementing IoT on a large scale in an industry as complex as banking is challenging. While the advantages and role of IoT in banking are clear and increasing with various studies, inadequate implementation of IoT can lead to potential risks and failures. This research aims to assess the banking industry's readiness for implementing IoT, specifically focusing on their IoT implementation readiness. The study identified the factors and aspects affecting the research topic using a systematic review method and classified its enablers into dimensions, components, indicators, and sub-indicators. After validating the initial model with experts, the final model revealed that 7 dimensions, 8 components, and 63 indicators influence the readiness of the banking industry to implement IoT. To rank the main aspects of the study, the Fuzzy SWARA method was used, and the results showed the following ranking: the dimensions of hard infrastructures, soft infrastructures, supply chain infrastructures, organizational factors, environmental factors, education and users, and security and privacy ranked first to seventh, respectively. The identified dimensions, components, and indicators provide a robust model for assessing the readiness of the banking industry for IoT implementation. The findings highlight the complexity involved in implementing IoT on a large scale within the banking sector.

1. Introduction

* mahmoud.zahediannezhad@mail.um.ac.ir
https://doi.org/10.59543/jidmis.v1i.12617

IoT is considered the third wave of development in the electronics and communications world after the Internet and mobile [1]. Its initial experiments and network expansion involved connecting to industrial equipment [2,3]. The concept was first introduced by Kevin Ashton in 1999 and was initially used in businesses to monitor the supply chain and logistics processes using the internet to track and identify products during transportation [4-6]. According to Gartner's annual survey of the technology Hype cycle, IoT is seen as a potential and growing technology. Its initial growth, acceptance, impact, and maturation are expected to take between 5 and 10 years [7]. Various associations, organizations, and companies are active in the field of IoT, each interpreting its role differently and providing different definitions of it [8,9]; Examples of such organizations include the Internet of Things Consortium, the IoT Association, the International Telecommunication Union (ITU), the European Telecommunication Standards Institute, the Institute of Electrical and Electronics Engineers [10], the IBM Institute, the Gartner Institute, the Cisco IoTG, the Internet Society, and others. For instance, according to the Internet Society (ISOC), by 2025, there will be 100 billion devices connected by IoT, and its economic impact on the world will be over $11 trillion [11]. The ITU considers IoT as one of the four advanced technologies in the field of ICT to develop an information and communication society [12]. Cisco has extended IoT into the Internet of Everything (IoE), which includes people, places, and things. In general, IoT comprises an ecosystem where various active technologies work together to shape the IoT value chain. These technologies include the internet, communication networks and protocols, standards, things and devices, sensors, cloud computing, big data, applications, and security and privacy [1,9,10,13,14]. These technologies are grouped into three categories: object-oriented (devices and sensors), internet-oriented (communication protocols and networks through the internet), and semantic-oriented (data analytics and knowledge) [13,14,15]. Each enabled-technology plays a role in the IoT ecosystem and has subsystems that businesses and industries must work together to provide [16]. Research have also investigated this issue. For example, some have examined the IoT ecosystem and its elements and factors affecting it [14,17]. Others studies have examined the assessment of IoT readiness in industries, businesses, and countries, highlighting the challenges ahead and the indicators affecting IoT implementation [10,18]. Additionally, other studies have depicted the applications and future of IoT in various industries, such as smart cities, smart manufacturing, banking, and more [6,19]. These challenges, factors, and indicators affecting IoT have forced businesses and industries to the assessment of their readiness to enter the IoT domain for successful implementation [5,10]. They assess their environmental readiness and business model with specific motivations and goals, and first define the indicators and factors affecting their business that is based on IoT [16,20]. Stakeholders and key actors are evaluated to develop proposed indicators, which are then used to determine the final set of indicators.

2. Research problem and question

Today, most businesses and countries are aware of the advantages of IoT and are actively seeking to integrate it into their infrastructure. However, the implementation of IoT requires careful consideration of the key components within its ecosystem and the challenges it presents. Prior to adopting IoT, it is crucial to assess the factors influencing this ecosystem, particularly the availability of both soft and hard infrastructures, which is referred to as "readiness." As defined by Parasuraman in 2000, technology readiness encompasses four fundamental principles that reflect how individuals and users respond to their preparedness for new technology or innovations. These principles emphasize the softer aspects of readiness, including trust, response mode, and attitude

(Parasuraman, 2000). Identifying and evaluating these dimensions can facilitate the adoption and implementation of new technologies. However, this is just one aspect of IoT readiness, and other influencing factors and dimensions must also be considered. Therefore, IoT readiness should be examined within a broader framework that encompasses various factors and dimensions impacting its implementation.

The intensity and impact of these factors may vary across different businesses and countries. By thoroughly analyzing the factors influencing the IoT ecosystem and identifying the dimensions that represent these influential factors—while also providing the necessary infrastructure—the full benefits and potential of IoT can be realized. Iran, with its recent advancements in ICT infrastructure, recognized by the International Telecommunications Union, and the emergence of startups and new businesses, holds significant potential for IoT implementation, particularly within its banking sector. However, the banking industry cannot hastily implement IoT without a well-thought-out strategy. This implementation requires consideration of technical and digital infrastructure, educational and financial resources, marketing strategies, organizational effectiveness, environmental factors, and, most importantly, the various actors within the IoT value chain. This process of review and assessment is commonly referred to as "readiness."

To successfully leverage IoT technology in banking, various aspects of its implementation must be considered, including ensuring security and privacy in IoT data transmission, establishing integrated databases, having a skilled pool of experts, creating user awareness, and developing comprehensive roadmaps. These factors contribute to different levels of readiness. Assessing this readiness becomes a critical step in implementing new technologies like IoT, particularly in developing countries such as Iran. Recognizing the significance of readiness, this research aims to assess the banking industry's readiness for IoT implementation and propose a model for conducting such assessments.

In addition, a key objective of this research is to apply advanced methods for ranking the main dimensions of IoT readiness in the banking industry. Specifically, the fuzzy SWARA method will be utilized to rank the dimensions based on their importance. This method will help in evaluating the intensity and impact of each factor, enabling the development of a comprehensive model for IoT readiness assessment. Thus, the research will address the following questions:

- What factors influence the banking industry's readiness for IoT implementation and how are they categorized across multiple dimensions?
- What are the indicators of the dimensions of the banking industry's readiness for IoT implementation?
- How can a model for IoT readiness in the banking industry be developed and implemented?
- How can the fuzzy SWARA method be applied to rank the dimensions of IoT readiness based on their relative importance?
- What is the relative importance of each dimension identified in the IoT readiness model when using the fuzzy SWARA method?

3. Research literature background

As stated in Section 2, the IoT has an ecosystem where its elements and subsystems work together, and the IoT value chain affects it so that the actors and stakeholders involved in it cooperate to guide this ecosystem into seamless connectivity. Various studies have investigated the IoT ecosystem, each introducing components that demonstrate a convergence between them. Table (1) shows the components of the IoT ecosystem in the research reviewed.

Table 1
The IoT ecosystem and its components from the perspective of research.

IoT ecosystem components	Ref.
Hardware, middleware and presentation, electronics (Microcontrollers and transceivers), software, sensors, actuators, and network connectivity, cloud computing, addressing schemes, data storage & analytics, visualization,	[17]
Compatibility, scalability, interoperability, and security, standardization of architectural, programming, communication, and cybersecurity	[21]
hardware and software platforms, computational resources, storing resources, disk resources, network resources, Application Programming Interface (API), Operating Systems (OS), Machine Learning applications	[22]
Devices, gateways, operating system, communication, middleware	[23]
Objects, Devices and Sensors, Stakeholders, Service Providers, Customers and Markets, Economic Factors	[2]
Semiconductors, Chips, Modules, Sensors, Platforms, Communication Networks, Services	[10]
Internet, Things, Sensors and Devices, Communication Networks, Applications, Network Virtualization, Cloud Networks, Cyber Physical Systems, Wireless Connections, Different Communication Protocols, Security and Privacy	[4]
Things & Sensors, Technical Infrastructures, Communication Networks, Wireless Connections, Metadata & Data Management, Software, Database	[6]
Reliability, interoperability, data localization, scalability, security and privacy	[24]
Identity management, discovery of resources, access tasking, vocabulary management, security management, charging	[25]
Internet, cloud computing, applications, communications networks, security and privacy	[9]
Objects, Devices, Smartphones, Tablets, Sensors, Wireless Communication Technologies, Communication Networks	[26]
Things & Sensors, Communications & Network, Cloud Space, Software, Mobile Ecosystem, Suppliers	[27]
IoT System (Uses & Application), Things and Objects, Sensors and Devices, Control & Operation of IoT Systems by Organizations, Service Providers, Customers, Markets	[28]
Heterogeneous Devices, Scalability, Data Exchange Using Wireless Technologies, Energy Optimization Solutions, Localization and things Tracking Abilities, Self-Organization Ability, Data Management and Semantic Interaction, Security and Privacy Mechanisms	[14]

Organizations and businesses must address IoT-enabled technologies by cooperating and integrating with their ecosystem. These technologies are like paradigms of computing (cloud, fog, and edge) for transferring and managing data from devices to data centers [29], Big Data (data advanced analytics technologies and algorithms) [30], Artificial Intelligence (tools for extracting and analyzing useful data and Increased security of data and information on gateway and network) [31,32], and Semantic technologies (such as WoT for displaying data to the end-user on web pages and monitoring devices and data at source). Research has also paid into this issue. For example, Wang & et al. [33] by presenting a model, by presenting a model, consider three IoT-related technologies for industries' readiness for IoT implementation, including the Internet of Everythings "IoE," (protocols required in the physical layer of IoT to communicate and connect among things), a cloud of things "CoT," (Cloud platforms for data collection and analysis them in the IoT application layer, using various analytical tools such as machine learning, data mining, and modeling) and web of things "WoT," (How to display and configure objects and status them through tracking, monitoring and remotely controlling them using web pages), which also security and privacy in these technologies is a major challenge for industries. In another study, Albishi & et al. [4], by exploring the IoT ecosystem, have identified emerging technologies for IoT that include cloud computing (for storing, editing,

managing, and processing data and information using multiple servers), semantic technologies (using semantic web-based formats in IoT), autonomy (Device Autonomy and real-time Behavior) and awareness (integration of devices and objects with the Internet to understand data collection and generated content), as key challenges and benefits of businesses in the future. Also, the International Telecommunication Union (ITU) (2017) has examined 4 technologies in ICT that are very closely related to each other, including IoT, big data, cloud computing, and artificial intelligence. They consider these four technologies, particularly the analytics of data generated from connections that lead to sustainable development in countries and business cooperation [12,34,35]. In addition, several studies have examined factors that influence the IoT ecosystem, categorizing them as drivers, enablers, dimensions, indicators, challenges, and solutions that have a significant impact on the implementation and deployment of IoT. These factors are intricately linked to the IoT value chain, either influencing it or being influenced by it. Table (2) provides an overview of the papers reviewed in this format, with the majority of them focusing directly on the factors and dimensions that affect the preparedness of the banking sector for IoT implementation.

Table 2
Factors affecting IoT readiness from various research perspective.

No.	Factors, Dimensions, Indicators, Constraints and Challenges Affecting IoT	Research Subject	Ref.
1	**Capabilities**: Integrated hardware and software facilities (Compatibility, Scalability, Efficiency and High Performance, Heterogeneous Connectivity, Interoperability, Operational Safety and Reliability;); Secure communication networks; Integrated internal and external networks; Integrated cloud services; High Security and Sensitive Information Protection; Flexible and Secure Identification Management and Communication; Customized Application Support; Reference Framework of Capabilities.	Industrial IoT Infrastructure and Smart Manufacturing	[3]
2	**Critical Success Factors:** Top management commitment; Organizational culture; Organizational readiness; Adaptability and agility	Critical success factors and Industry 4.0 for organization	[16]
3	**Challenges:** IoT privacy and security; Customer privacy; Training users specially to enhance their safety; Secure data sharing; Heterogeneity in devices	IoT diffusion in smart stores	[5]
4	**Factors**: Personal privacy; Public safety; Industrial security; Dubious data gathering; Systemic governance approach; IoT innovation system; Scope of IoT governance; Policymaking; ICT infrastructures; Regulatory and Legitimation; Service Provision and Facilitation; Knowledge Development & Diffusion; Resource Mobilization; Market Formation; Direction of Research.	Governance and Key Processes of IoT Innovation System	[15]
5	**Factors**: Customer needs; Integrated systems; Device interoperability; Safety of devices	IoT integration in supply chain management	[36]
6	**Indicators**: People and capacity development; Organization, policy and cooperation; Process management; Technology and technical; Legislation and regulation; Organizational Training; Risk and Opportunity Management; Managing Performance; Monitor and Control; Governance; Requirement Development and Management; Configuration Management; Process Management; Implementation Infrastructure; Technical Solution; Service Delivery Management; Strategic Service Management.	Maturity and readiness industrial 4.0	[37]
7	**Factors:** Competitiveness among stakeholders; Governance of data security; Strengthening IoT readiness; Guarding the privacy; Diffusion and upgrading of IoT; The volatility of online data; Lack of responsibility and accountability	Governing the progress of IoT	[38]

	of corporations; Policies (privacy-by-design and citizen-centric regulation); Protect the interests of IoT users.		
8	**Factors**: Planning, Operability, Awareness, Responsibility, Manpower, Financial, Equipment, Legal, Training, Infrastructure, Devices & Tools.	Readiness Framework in IoT Forensics	[39]
9	**Factors:** Perspectives of Human, Technology, Governance and Management, Security Perspective, Policy and Law.	IoT Readiness in Public Organization	[40]
10	**Factors:** Aspects of social, cultural, human, technological, financial, managerial, government rules and regulations.	IoT Readiness Level	[41]
11	**Factors and Challenges**: Size of the manufacturing firms; The significant amount of capital investment; Knowledge and training of users; Strategic managerial approach; Qualified human resources; Lack of a collaborative strategy for digitalization; Require awareness and readiness for IoT; Acquiring and sharing a comprehensive up-to-date knowledge of technology; Collaborative efforts of all members of supply chains; Relationships between unions, policymakers, researchers, and stakeholders.	Awareness and readiness of Industry 4.0	[42]
12	**Challenges:** Securing environment components; Improper device updates; Lack of efficient and robust security protocols; User unawareness; Active device monitoring; Security and privacy issues and threats	Security and privacy in IoT	[43]
13	**Factors & Challenges**: Components: Enhanced security, Physical infrastructures and systems, Smart Applications, Cloud Computing involvement, Proprietary hardware and software, data analytics, Standardization of IoT platform	IoT Digital Forensics Readiness	[44]
14	**Factors**: New business model, Demand response services, Customers' attitudes, Infrastructure development, Technical support, Network infrastructure, Measurement infrastructures, Information infrastructure, Security systems, Human Resources, Cost structure, Revenue streams.	Consumer readiness for participation in IoT	[45]
15	**Factors & Challenges**: Government support, Organizational and financial aspects, Means and resources for training, HR and skill development policies, strategies, and plans, Users' training, Data privacy.	IoT in SMEs and Industry 4.0	[46]
16	**Dimensions**: Organizational and environmental culture	Hofstede dimensions on IoT readiness implementation	[47]
17	**Factors**: Security, Networking, Software Development, Regulations, User Intention, Efficiency	Employees' readiness to IoT applications	[48]
18	**drivers**: Leadership (success, competence, experience, technical expertise, and leadership abilities; strategic thinking and management system; alignment with different perspectives and plans; Trust building and the frequent involvement of the management system with stakeholders), self-efficacy (Project team abilities and competencies) and environmental factors (environment of national, international, social, cultural, economic and political) **Enablers**: Government, Policymakers, Financing Agencies, Informal Groups, and Stakeholders	drivers of Implementation readiness of ICT Projects	[49]
19	ICT infrastructure, the use of communication networks (such as mobile and mobile internet access between users and customers in terms of data traffic and download speeds), Big data maturity and data analytics, Communication platforms such as cloud computing and communication devices such as automated and connected processes, Having experts and staff with the necessary skills, And public policymakers and resource allocation	Industry 4.0 Readiness	[50]
20	Technical / Technology Dimensions (Hard and Soft Infrastructure in Different Technologies), Understand the Potential Benefits and Understand of	Smart City Readiness	[51]

	livability, Regional and National Policies, Various Stakeholders such as Government, Industry, and Experts		
21	Number of mobile subscribers, mobile broadband connections such as 3G, 4G, and 5G, ownership of smart mobile devices, SIM penetration and operators' investment in mobile and ICT infrastructure	Role of mobile operators and ecosystems in IoT development	[52]
22	**Factors**: Sensor devices and things, beneficiaries that manage system activity, service providers, customers and markets (suppliers, manufacturers, mobile operators), economic factors **Restrictions**: Mutual standards and infrastructure such as penetration and public access to the Internet, ICT and IT infrastructures, security and safety, socio-cultural factors such as culture and privacy, government policies, and the age groups population.	IoT readiness and factors affecting its ecosystem	[2]
23	Technical and organizational and cultural dimensions (hardware and software infrastructure, network conditions, strategy and organization, human resources and organizational culture) **Factors**: Stakeholder involvement and the size of the business	Smart Manufacturing Readiness in Industry 4.0	[53]
24	**Dimensions**: Strategy, Leadership, Customers, Products, Operations, Culture, People, Governance, Technology and Development Team	Smart manufacturing system readiness	[54]
25	**Dimensions**: Organizational, Data analytics, IT Infrastructure, Team expertise, Leadership, Network technologies, Data integration, Team experience, Strategy (business models, processes), Storage technologies, Governance, Security Techniques	IoT Readiness	[55]
26	**Factors**: Access to appropriate physical infrastructure, including devices, networks, data storage, and processing; Basic services such as connections, computing services, and data transmission channels; User knowledge and skills; Policies adopted to develop sustainable and scalable solutions	Role of Advanced ICTs in Sustainable Development	[11]
27	**Indicator**: Development and deployment of cloud (private and public) models, data usage (including data sources, data flow and control, and data centers), data advanced analytics, risk management, and governance	IT Infrastructure Readiness for IoT in Business	[56]
28	Customer understanding and IoT ecosystem interaction with the business model, data analytics	IoT readiness and business	[6]
29	Security and privacy	Security and privacy in IoT	[57]
30	Businesses understanding of the IoT, how to the structure of the business, partnerships between IoT infrastructures suppliers, sales and supply of manufactured parts at reasonable prices by suppliers, and international collaborations	Using IoT innovations in SMEs	[10]
31	**Institutions factors, supply-side factors and demand-side factors**: (The role of domestic companies and their partnerships in providing infrastructure, university and IoT specialists' relationship with industry, cooperation between domestic and foreign industries, organizational factors, mobile operators and competitiveness between them by the government, skills and training, local infrastructure, legal and illegal effects, compatibility with social roles such as privacy, government policies, strategies, and incentives, political controls, size and market need and deployment costs)	The evolution of the IoT industry and market	[13]
32	**Challenges**: Planning, careful management and supervision/ monitoring, promotion of knowledge and skill, having experts, ICT and Non-ICT Infrastructures, data and Information management, security and privacy and IoT ecosystem actors	IoT readiness	[58]

33	**Dimensions**: Social and Economic; **Challenges**: Policy and Technology **Indicators**: reliability, interoperability, data localization, scalability, security and privacy in relation to the IoT ecosystem, bandwidth range level, legal impacts, access and cost of internet connection, access to data and data centers, Smart device ownership, cloud space usage, communication networks, training and skill Solutions: Reduce Internet tariffs, Understanding the use of smart devices, offering capacity-based discounts, Enhance bandwidth, Ability to Store and processing data, Providing mechanisms to increase security and privacy, Adopt policies regarding IoT implementation and deployment, Customer and community awareness, and usefulness understanding of IoT usage	IoT Implementation Indicators	[24]
34	IoT-based business model, data analytics, data and information security, technical infrastructure, privacy	Security and privacy in IoT and IoT-based business changes	[26]
35	**Indicators**: Environment, Readiness, Use, Impact **Sub-indicators**: (laws and regulations, type of business, quality of management practices, networks of communication and mobile, quality and availability of broadband, education/ training, skill, experts, economic and social impacts, government role and support, Suppliers)	Network Readiness Index (NRI), ICT Status Assessment	[59]
36	**Dimensions**: Strategy, Leadership, Customers, Products, Operations, Culture, People, Governance and Technology	Readiness and Maturity of Industry 4.0	[60]
37	Environmental and strategic elements, IoT-based business model, technology infrastructure availability, information and data management, suppliers	IoT in developing countries	[27]
38	**Challenges and Factors**: Physical and Social Infrastructure, lack of energy, Internet access and bandwidth, network Infrastructures, Deployment costs (Purchase of equipment and investment by companies) and business challenges, collaborations Public-Private sector together, and the creation of competition among the domestic companies by the government	IoT readiness	[28]

Studies have delved into the impact of IoT on banking, specifically, the factors that influence its implementation and the difficulties that arise. Dineshreddy & Gangadharan [61] have presented an IoT-based financial services system framework. The framework consists of 5 layers. The first layer, the "Physical Device Management Layer," includes various devices embedded with the sensor; "Communication layer" refers to the database and cloud space for sending data; "Communication layer" refers to the database and cloud space for sending data; The "integration layer" is about data integration and the use of different tools of data storage, integration, and interaction; The "analytics and processing layer" includes all such actions as, processing and analytics data and using IoT intelligence with various tools such as BI, and the last layer is the "application layer," which relates to applications and use by end-user. Rimer [61] has presented an IoT architecture for financial services in developing countries. With this architecture model, banks can take advantage of IoT applications and reduce banks' investment in remote areas, theft, fraud, and money laundering, and increase security and privacy. This architecture model has three main components (platform), data transfer (edge platform), data storage and processing (IoT platform), and data analytics (enterprise IoT platform) that are associated with a variety of communication channels. IoT platforms in these three components consist of databases, hardware and software systems, and cloud computing, and this model's basic architecture requires using NFC devices for transactions. Del Giudice & et al. [63]

have investigated the Bank of Things "BoT." They have compared banks using IoT to traditional banks. Research considers IoT-based mobile services very important for banks' competitiveness in the future. To create a competitive advantage and take advantage of IoT, IoT-based banks should consider investing in two sectors. First, they manage the IoT-based financial services process, and second, they build partnerships with cloud services providers. Boumlik & Bahaj [64] have examined the role of Big data and IoT in banking services. They have developed an architectural model for fraud detection using IoT and technologies related to Big data, namely "Hadoop" and "Map-reduce," which include three layers. The "resource layer" includes using IoT technology to collect data across multiple channels, devices, and things in the form of online and offline. The "big data layer" is the use of the "Hadoop" framework and the "Map-reduce" model to discover and understand fraud patterns and methods. The "application layer" uses fraud modules and processed data to understand and identify fraud patterns; Research suggests that real-time transaction data is the best solution to detect fraud in the banking system. conducted a study examining the utilization of smart bank cards within Russian financial institutions. Through a case study of the "largest Russian bank," the findings revealed that the implementation of smart cards proves to be significantly more effective in larger banks compared to smaller ones. It not only reduces instances of financial theft but also enhances the security of both customers and the banking system as a whole. However, adopting these smart cards necessitates substantial costs associated with replacing plastic cards and modernizing ATMs, which require substantial financial resources and support from both the public and private sectors [65]. Saxena & Al-Tamimi [66] have examined the role of IoT and Big Data technologies in the bank. By reviewing and evaluating four banks in Oman, they consider challenges such as high costs to reform and build R&D infrastructures and obstacles such as organizational barriers (Regulations, Standards, Trust, and Security), structure and existing processes (Such as the obstacles to rebuilding existing business networks and creating new business models) part of the challenges and barriers IoT implementation. In order to overcome these barriers, the banking sector needs to take into account several key factors. These include staff training, security and privacy needs, the institutionalization of IT infrastructure, changing the business model, investing time and resources, collaborating between internal and external stakeholders (such as government, university, and other businesses to address technical challenges), government policies, adopting and applying policy and legal mechanisms, and the attention to R&D infrastructure. In their view, merging these two technologies and using Self-Service technologies can predict customer behavior, increase bank productivity, and gain customer confidence. Schimek (2016), considers the use of innovations from emerging technologies such as IoT, require to provide R&D areas, and banks need to make efforts to innovate in their R&D labs, which include researches, plans, prototypes, and pilot of products and services [67].

3. Research methodology

The dimensions, components, and indicators in this study were derived through a systematic review method, which involved a comprehensive analysis of existing literature to identify the key factors influencing IoT readiness in the banking industry. After extracting these dimensions and their corresponding components, the next step focuses on assigning weights and ranking the importance of these dimensions. This ranking process will be carried out using the fuzzy SWARA method, which is specifically applied to the dimensions of the model. In the following subsections, both the systematic review method and the fuzzy SWARA technique will be explained in detail to provide a comprehensive understanding of how these methods contribute to the assessment of IoT readiness in the banking industry.

3.1. Systematic Review Methodology

The current research aims to provide a model for the banking industry's readiness to implement IoT. For this purpose, a Systematic Review approach is chosen. "Systematic review" is a tool for identifying, evaluating, and interpreting all existing research about a particular research question, subject area, or phenomenon of interest. A systematic review is conducted to provide a fair assessment of a research topic using a trustworthy, accurate, and reliable methodology. Kitchenham [68], to do a "systematic review," says: One must first consider mechanisms for gathering evidence from different studies and then understand how much evidence could be relied on to cover the research questions. She provides guidelines for a systematic review that comprises three main phases: 1) Planning the review, 2) Conducting the review, and 3) Reporting the review. Each of these phases has stages that include: The first phase consists of the steps: (1- identifying the requirements for a review and 2- developing a protocol for the review); the second phase includes the steps: (1- Identification of research, 2- Selection of primary studies or research, 3- assessment of the quality of study or research, 4- Monitoring and extraction of data and information, and 5- Synthesis of data and information) and last phase is a single-stage phase [69,70,71].

In this research, following these steps have adopted the method used in the research [72]. At first, six databases and scientific sites were identified in English, and a search was done with a set of predefined keywords, and the initial search resulted in 360 research titles. Then, trivial research resources (articles, books, reports) were removed when reviewing the titles, keywords, abstracts, and full-text reviews. After an in-depth study of the research sources, they were classified into 4 groups, and the relevant data were extracted from the research sources in each group. The following steps illustrate these actions:

3.1.1. Searching for resources

First, the following 6 databases and scientific websites were selected in English and were searched:

“Google Scholar”, “Scopus”, “ScienceDirect: Elsevier”, “Springer & Kluwer”, “Emerald”, and “IEEE”.

3.1.2 Keywords

Given the keywords related to the research, "IoT readiness" and "IoT in the Bank," and various searches in different scientific databases, the keyword range that was related to the research topic and made special help in solving the research problem was expanded, as shown in Table (3):

Table 3
Searched terms in English scientific databases (keywords)

Readiness of IoT/ Internet of things	Internet of things /IoT readiness
Readiness of countries for the Internet of things	Readiness for IoT/ Internet of things
Internet of things /IoT implementation	Implementation of IoT/ Internet of Things
IoT in the bank/Banking	IoT and Banking/Bank
IoT in financial services	IoT in the Service industries
Bank’s readiness for internet of things/IoT	Industry’s readiness for internet of things/IoT
IoT/ Internet of Things readiness assessment	Industry 4.0 readiness
IoT Challenges and Applications	IoT and Industry 4.0

3.1.3 Inclusion / Exclusion Process

Initial search for the top terms resulted in 300 research titles that were categorized into 4 categories: "Challenges, Factors, and Dimensions Affecting IoT," "IoT Readiness," "Electronic Readiness," and "IoT in Banking." The titles on an Excel sheet and resources in the Mendeley Software Database were stored for management. Initially, documents that were irrelevant to the research topic (100 titles) and duplicates (40 titles) were removed. To this end, research sources that did not match the keywords listed above related to the research topic were removed and limited to 160 research sources. Subsequently, 52 sources were removed by reviewing the abstract and conclusion of research sources unrelated to the four main areas. At this step, the criterion for resource deletion is based on mismatches with areas that do not fall into the four main areas, which are, 1) IoT ecosystem and applications, challenges, dimensions, and indicators affecting IoT in the "Factors affecting IoT" category; 2) IoT readiness and related areas such as Industry 4.0, smart city, intelligent manufacturing and big data and IoT implementation in the "IoT readiness" category; 3) Technology Readiness Levels, Technology Readiness Indicators, E-Government Readiness, E-Banking Readiness, Digital Readiness, and ICT Readiness Indicators in the category of "Electronic Readiness," and 4) IoT applications in the bank, Implementation of IoT in the bank, mobile banking, NFC and RFID applications in the bank, payment systems, financial services, and digital banking in the "Internet of Things in Banking" category.

In the following, the remaining 108 sources were examined for the full text in terms of introduction and methodology, and at this stage, 88 filtered sources and 20 other sources that, in terms of reviewing the full text, were not aligned with the research topic were excluded. Finally, the remaining research resources were re-reviewed to form the final set of resources for the subject of the research analysis. The main criterion for selecting the relevant sources is based on the domains mentioned in the upper four categories. For this reason, research sources that did not cover these four categories were rejected while their full text was reviewed. These 88 sources are directly and indirectly involved in the subject area of the research and provide an appropriate roadmap for answering the research questions. But the main basis of the research consists of 55 final sources that cover the dimensions, indicators, variables, factors, models, frameworks, and architectures that are effective on "Readiness of IoT and its applications in banking," and most of the components of the research model have been extracted from them. But 33 other sources cannot be trivial. Table 4 shows the process of Inclusion / Exclusion of research resources:

Table 4
process of Inclusion / Exclusion research resources

Process	Number of documents deleted	Number of documents remaining
primary list of Research Resources	0	300
the Delete based on title and keyword	140	160
the Delete based on abstract and conclusion	52	108
the Delete based on full text	20	88
Modification based on the main base of research	33	55+33
Final List	----	55

Figure 1 also shows the frequency of research resources available in 11 areas, including A) “Vision, Challenges, Opportunities, Applications, Solutions, Strategy and Future of IoT”; B) “IoT and Related Technologies in Banking and Payment Systems”; C) “IoT readiness and related indicators”; D) “Industry 4.0 readiness “; E) “Security and Privacy Issues and Challenges in IoT”; F (“IoT Implementation Models and Frameworks”; G) “Digital readiness”; H) “ICT and ICT Readiness”; M) “Other Documents.”

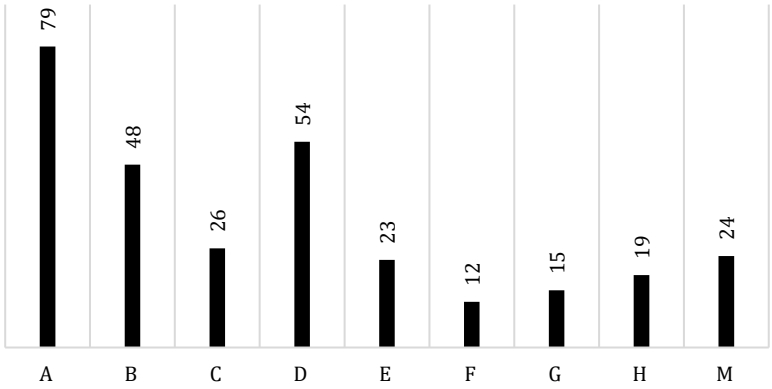

Fig. 1. Frequency of categorization of reviewed research sources

After reviewing previous research, the research hypotheses (Dimensions, Components, Indicators, and Subheads), or in other words, the enablers, were determined that the initial model consists of 7 dimensions, 8 components, and 68 indicators. These components were then evaluated in a questionnaire format by 8 experts for model validation. Expert panel members include academic experts in IT and IoT who are familiar with IoT technology and management concepts, as well as work and scientific experience. Lawshe test (Content validity check using relative content validity coefficient "CVR") [73] and binomial test (in non-parametric statistics) were used to assess the validity of the model. Due to limited space, these analyzes have yet to be included in the research. The analysis results show that all 7 dimensions and 8 components were accepted, but out of 68 indicators, 5 were not approved. Figure 2 shows the final research model. In Figure 3, large circles, hexagons, and small circles represent the dimensions, components of each dimension, and indicators of the model, respectively, in which the numbers inside represent the number of corresponding elements.

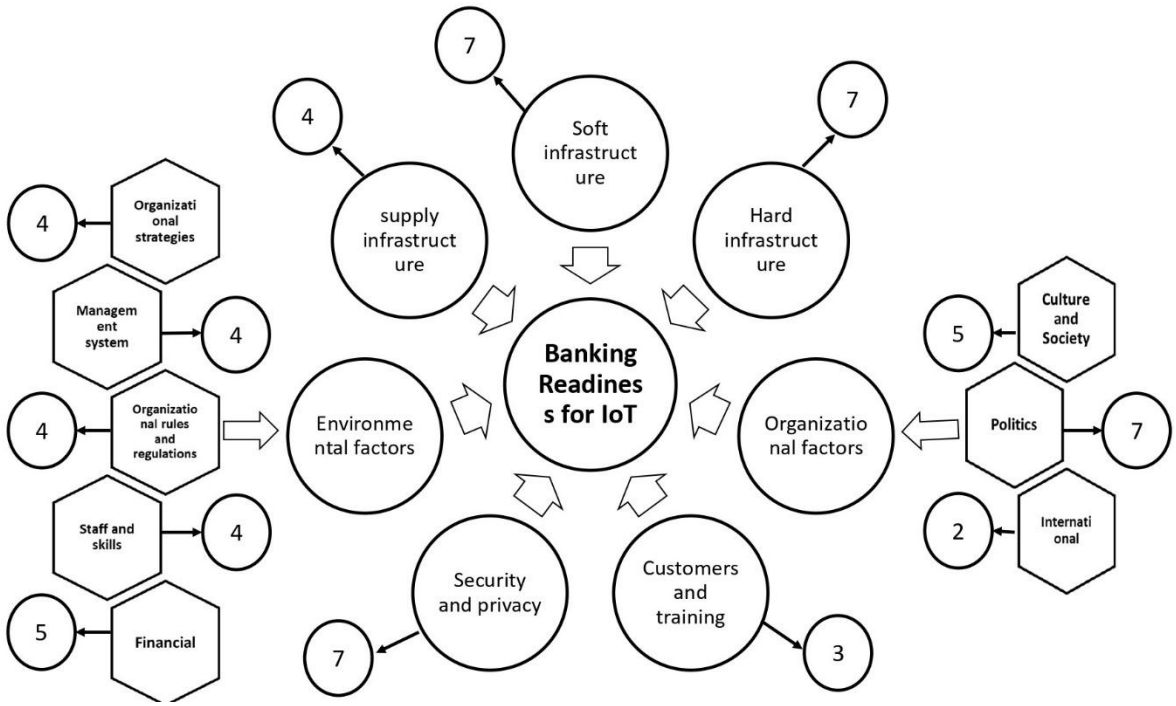

Fig. 2. The final model of IoT implementation readiness assessment in the banking industry

Table 5 shows the frequency of 7 dimensions of research in previous research:

Table 5

Frequency of dimensions used for the research model in terms of the previous research.

Authors	Dimensions						
	SI*	HI*	EF*	OF*	CT*	SUI*	SP*
[3]	✓	✓					✓
[16]				✓			
[5]	✓				✓		✓
[36]		✓			✓		✓
[15]			✓	✓		✓	✓
[37]	✓	✓	✓	✓	✓		
[38]			✓	✓		✓	✓
[39]		✓	✓	✓	✓		
[40]	✓	✓	✓	✓			✓
[41]	✓	✓	✓	✓			
[42]			✓	✓	✓	✓	
[43]		✓			✓		✓
[44]	✓	✓					✓
[45]	✓	✓		✓	✓		✓
[46]			✓	✓	✓		✓
[47]			✓	✓			
[48]	✓	✓	✓		✓		✓
[50]	✓	✓	✓	✓		✓	
[49]			✓	✓		✓	
[33]	✓	✓					✓
[2]	✓	✓	✓	✓	✓	✓	✓
[53]	✓	✓		✓		✓	
[51]	✓	✓	✓	✓	✓	✓	
[55]	✓	✓		✓			✓
[64]	✓	✓					

[65]			✓	✓		✓	
[52]		✓				✓	
[54]	✓	✓	✓	✓	✓	✓	
[56]	✓	✓		✓			
[4]	✓	✓					✓
[6]	✓	✓		✓	✓		
[57]				✓			✓
[10]	✓	✓	✓	✓		✓	
[13]		✓	✓	✓	✓	✓	✓
[12]	✓	✓	✓	✓	✓	✓	✓
[66]	✓	✓	✓	✓	✓	✓	✓
[58]	✓	✓		✓		✓	✓
[61]	✓	✓					
[24]	✓	✓	✓	✓	✓		✓
[67]				✓			
[59]	✓	✓	✓	✓	✓		
[61]	✓	✓					✓
[26]	✓	✓	✓				✓
[60]	✓	✓	✓	✓	✓	✓	
[27]	✓	✓	✓			✓	
[28]		✓	✓			✓	
[14]	✓	✓					✓
Our Study	✓	✓	✓	✓	✓	✓	✓

* Soft infrastructure (SI)
* Environmental Factors (EF)
* Customers and Training (CT)
* Security and Privacy (SP)
* Hard infrastructure (HI)
* Organizational Factors (OF)
* Supply Infrastructure (SUI)

3.2. Fuzzy Stepwise Weight Assessment Ratio Analysis (SWARA) Method

Fuzzy methods and decision making are used in many studies [74,75,76,77,78], one of which is fuzzy SWARA. In this study, the Fuzzy SWARA method is used due to its capability to handle ambiguous and uncertain data. Decision-making in complex, multi-criteria environments is often confronted with challenges such as imprecision and uncertainty in evaluations [79,80,81,82]. The fuzzy SWARA method, by combining expert opinions and fuzzy logic, enables the effective processing and analysis of expert assessments, which are often expressed in the form of fuzzy and uncertain data. The fuzzy SWARA method is particularly efficient in problems where criteria and options are characterized by uncertainty and ambiguity, allowing researchers to prioritize options more accurately and make better-informed decisions. The steps of the fuzzy SWARA method are as follows [74]:

Step 1: Identifying Dimensions

In the first step of this research, the dimensions were extracted using the Systematic Literature Review method. The SLR method, by combining results from various studies and integrating existing information, provides a comprehensive and reliable view of the different dimensions, which is critical to the precision of the fuzzy SWARA method.

Step 2: Collecting Expert Opinions

In the second step, expert opinions from the academic field were collected. These experts had significant expertise and experience in the fields of information technology and information systems, and their opinions were utilized to enhance the accuracy and credibility of the analysis results. A precise and systematic process was followed to select the final experts, where 10 individuals with the required qualifications and scientific competence in this area were chosen. These qualifications included practical experience in relevant fields of information technology, active participation in research and academic projects, and the ability to analyze complex issues within information systems. The goal of selecting these experts was to ensure the validity and reliability of the research results and to achieve accurate scientific and practical analyses that contribute to better decision-making in this domain.

Step 3: Integrating Expert Opinions

The expert opinions were integrated using Formula 1. In this formula, M represents a fuzzy triangular number, and k is the number of experts.

$$\tilde{G}_{i,j-1} = \frac{\sum_{i=1}^{k} \widetilde{M}_{i,j-1,k}}{k} \quad (1)$$

The sum of two fuzzy triangular numbers is calculated using Formula 2.

$$\widetilde{M}_1 + \widetilde{M}_2 = (l1 + l1, m1 + m2, u1 + u2) \quad (2)$$

Step 4: Defuzzification

In this step, the indicators are defuzzified using the following formula, and are examined along with the fuzzy data.

$$D_{ij} = \frac{u_{ij} - I_{ij} + m_{ij} - I_{ij}}{3} + I_{ij} \quad (3)$$

Step 5: Calculating the Growth Rate

The indicators are arranged in descending order based on their defuzzied values. Then, the difference between each indicator and the preceding one is calculated, denoted as Sj. Subsequently, the growth rate for factor j is calculated based on Formula 4. For the first factor, this growth rate is assumed to be equal to one by default.

$$k_j = \begin{cases} 1 & j = 1 \\ s_j \oplus 1 & j > 1 \end{cases} \quad (4)$$

Step 6: Calculating the Key Factor Importance

This indicator is derived from Formula 5, where, by default, the importance coefficient for the first factor is assumed to be one.

$$q_j = \begin{cases} 1 & j = 1 \\ \dfrac{q_j - 1}{k_j} & j > 1 \end{cases} \quad (5)$$

Step 7: Calculating the Relative Weight

The fuzzy relative weight for each key factor is calculated separately using Formula 6.

$$w_j = \frac{q_j}{\sum_{j-1}^{n} q_j} \quad (6)$$

Step 8: Defuzzification of Relative Weights

The crisp weight for each factor is determined using Formula 7. These weights represent the final ranking.

$$D_{ij} = \frac{(w_{uj} - w_{lj}) + (w_{mj} - w_{lj})}{3} + w_{lj} \quad (7)$$

4. Research findings

The future of banking is heavily influenced by technological advancements such as AI, IoT, and digitalization. As noted by Ashayeri et al. (2024), these innovations are reshaping customer engagement and service delivery, opening new opportunities for growth. The integration of IoT in banking enhances operational efficiency and supports more personalized services. These technologies align with the need for robust infrastructures, both hard and soft, enabling banks to stay competitive and meet evolving customer demands [83]. In terms of methodology, evaluation, and comparison of the quality of review research shows, studies focusing on the challenge, vision, application, and future of the IoT have focused more on the hardware, software, and security aspects of the IoT, which they consider the preparation and attention to these components to be the cause of the realization of the Internet of Things [4,14,15,16,26]. And other studies that have discussed IoT readiness, factors, and indicators affecting IoT and IoT applications in the bank, such as [2,3,5,6,10,11,13,24,27]. show that in addition to the readiness of hard and soft infrastructure and increased security and privacy in the IoT ecosystem, different actors and stakeholders in this ecosystem should be considered. By combining and summarizing these studies, it can be understood that the factors that affect the readiness of the Internet of Things in banking can be classified into 7 dimensions, which are: "Soft Infrastructure (Software, applications, platforms, databases and data analytics)," "Hard Infrastructure "(Hardware, network, devices, internet), "Environmental Factors," "Organizational Factors," "Customers and Training," "Supply Infrastructure (Suppliers and service providers)" and "Security and Privacy." Eight components, 67 indicators, and 4 sub-indicator, in addition to these 7 dimensions, affect the readiness of the IoT in banking, Which includes three components "culture and society," "politics (laws, regulations, and government)" and "international" in the dimension of "environment," and the five components of "organizational strategies," "management system," "rules and regulations of the organization (standards, monitoring, and evaluation)," "staff and skills" and "finance" in the dimension of "organization." This section focuses on the dimensions of the research model and discusses the results obtained.

4.1. Dimension of hard infrastructure (hardware, network, devices, internet)

Hardware infrastructure can be considered the main foundation of the IoT ecosystem, which is of special importance in the four layers of the IoT, namely "physical," "network," "integration," and "application," its special role is more prominent in the physical (device) and network layers [3,36]. Figure 3 shows the indicators of this dimension. As Wang et al. [33] point out, the industry's attention

to the three technologies "IoE," "CoT" and "WoT" is important for IoT implementation. The profitability and efficiency of banking infrastructures, such as IoT- based ATMs, can significantly benefit from predictive models and data-driven decision-making. The banking industry should also pay special attention and invest in "quality, high-speed and secure communication networks," "ensuring the secure connection of objects and devices to collect data," "Providing secure cloud infrastructure for collecting and storing, transmitting and analyzing data obtained and computations on them," "Providing multiple and integrated databases to collect big data for data analytics," and measure the readiness of their business in this infrastructure.

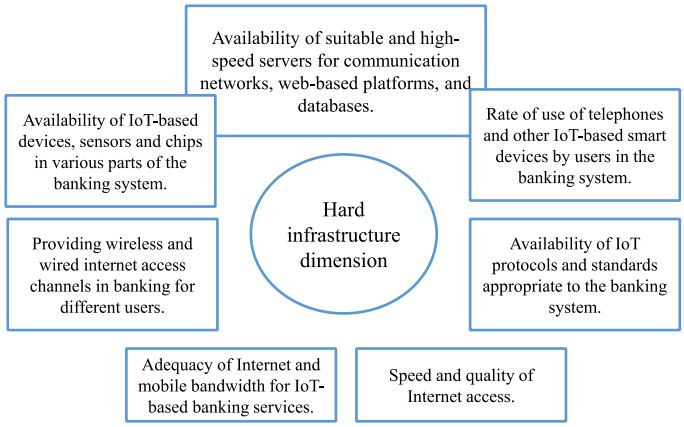

Fig. 3. Indicators of hard infrastructure dimension

4.2. Dimensions of soft infrastructure (software, applications, platforms, databases, and data analytics)

Soft infrastructure is closely related to hard infrastructure and, like hard infrastructure, plays a special role in the four layers of the IoT. The most important difference between these two dimensions is that this dimension refers more to the application layer, which can analyze data with artificial intelligence and big data tools. Their main common point is in the integration layer. Data is collected by objects and devices (in hard infrastructure) and various platforms (in soft infrastructure) and stored in databases and cloud space [3,5]. The readiness of the banking industry for IoT implementation relies heavily on advancements in soft infrastructures. Silicon Valley's technological innovations, such as advancements in AI and microprocessor technologies, provide a roadmap for improving operational efficiency and scalability in banking systems. Figure 4 shows the indicators of this dimension. The banking industry should evaluate the components involved in this infrastructure before implementing IoT in their business structure and model because experience shows that a Lack of readiness in the technical infrastructure is one of the reasons for the failure of IoT implementation.

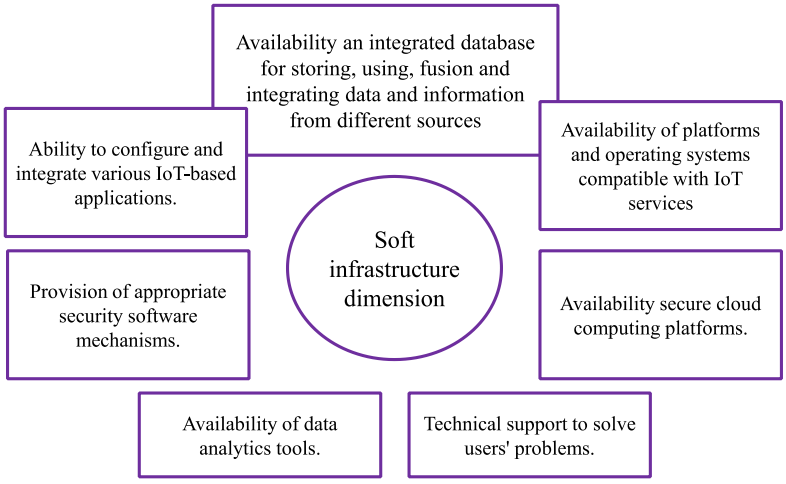

Fig. 4. Indicators of soft infrastructure dimension

4.3. Environment dimension

The environment of a business is defined based on its constituent elements. These elements can affect a business or be influenced by it. The entry of the banking industry into the IoT is no exception. Several factors in this dimension can affect the implementation and realization of the IoT. Several studies have pointed to these factors, including: 'International cooperation between domestic and foreign companies' [10], 'Illegal and legal influences, government policies, international cooperation, political controls, market size, and needs' [13], 'Cultural and social factors' [2], 'Government policies for IoT investment by the public and private sectors' [28], 'Social and economic dimensions' [24], 'Public policymakers' [50], 'Regulators, government policies and the adoption of laws and their effects' [12], 'Social and legal concerns about data usage' [26,41]. Environmental factors significantly influence the readiness of the banking sector for IoT implementation. Insights derived from social media discourse have been shown to impact decision-making processes in government agencies [84]. Understanding the environment and the banking industry's readiness to respond to environmental impacts can facilitate IoT implementation. Considering the review of previous studies, this study considers three components effective in the environmental dimension. These components have discussed below:

4.3.1. Culture and community component

Government and organizational structure play a critical role in the cultural and social factors influencing IoT implementation [41,46]. To implement IoT in banking, relevant government agencies must first familiarize users with the concepts and benefits of IoT and create a strong cultural background before using IoT with multimedia tools. Figure 5 shows the indicators of this component.

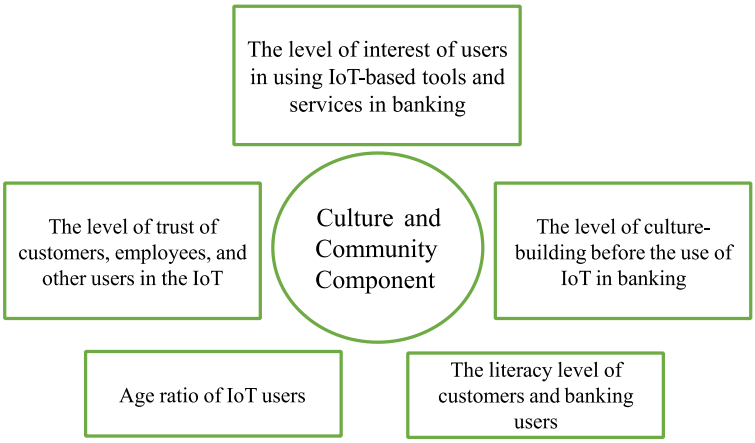

Fig. 5. Indicators of culture and community component

4.3.2. Policy component (laws, regulations, and government)

The International Telecommunication Union considers one of the four main factors in the understanding of technologies such as IoT by countries and businesses to be the adoption of policies and guidelines to develop sustainable and scalable solutions [12]. Government policies in enacting and adjusting laws, creating market competition, incentives and budgets allocated, and providing key infrastructure can be challenges and political factors influencing the implementation of the IoT. By creating a framework, government agencies can adopt general policies for IoT implementation, and regulators and the banking system can facilitate IoT implementation by considering this framework. The indicators in Figure 7 can determine the government's influences in various ways on the implementation of IoT in banking:

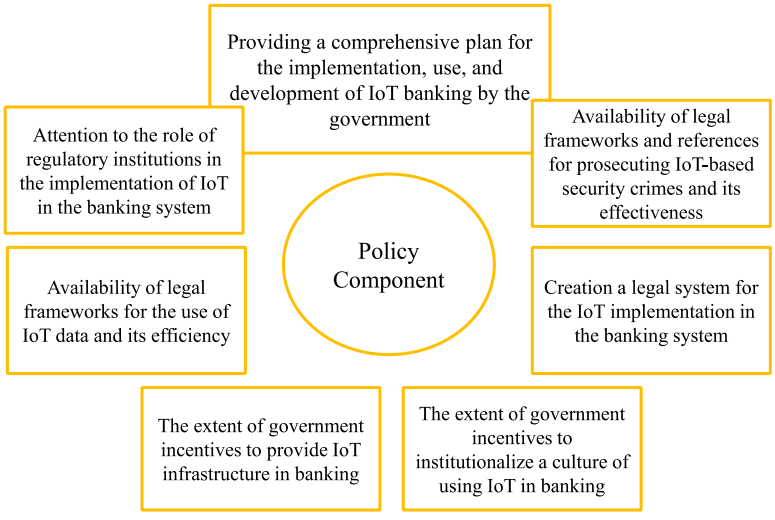

Fig. 6. Indicators of policy component

4.3.3. International component

Several studies have pointed to the cooperation of domestic and foreign companies to provide components to the IoT ecosystem in businesses. For example, some studies have focused on approaches such as suppliers and domestic producers to produce and supply soft infrastructure, and

on approaches such as imports, partnerships, and international investment to provide hard infrastructure [13,28]. Banking industry policymakers should consider which domestic and foreign suppliers are appropriate for their industry to provide the equipment needed to implement IoT [85]. Because sometimes the supply of equipment by foreign companies may be cheaper than their production in the environment in which the banking industry operates. The indicators in Figure 7 can well describe this component.

Fig. 7. Indicators of the international component

4.4. Organizational dimension

In addition to the macro-environment, policymakers in the banking industry should also consider the micro-environment or the internal environment of their business, and not look at their organization with an "everything good" view. From the organizational point of view, factors such as strategies, setting and adjusting of organizational rules and regulations, management system, staff and necessary skills and financial issues also affect the implementation of IoT. There are several factors in this dimension that can affect the implementation of the IoT. Several studies have pointed to these factors, including: 'Impact of organizational rules, skills and training' [13], 'Economic factors' [2], 'Strategies, planning, careful management and monitoring, training and presence of experts' [40,58], 'Establishment costs' [28], 'Adopted organizational policies and training and skills' [24]. Several studies have also pointed to the organization's focus on the IoT-based business model, such as model structure, new model creation, and change [6,16,26]. The following are five components that affect the organizational dimension of IoT implementation:

4.4.1. Component of organizational policies and strategies

IoT developers and managers in the banking industry, in addition to reviewing and analyzing benchmarks and increasing R&D programs theoretically, need to create an appropriate roadmap (Setting policies, strategies, goals) to steer their business model toward practical IoT implementation activities [48]. By examining these analyzes, they will find out which IoT projects are appropriate for their business model for investment. Figure 8 shows the indicators of this component. Recognition and study of these indicators can be a good understanding of this component.

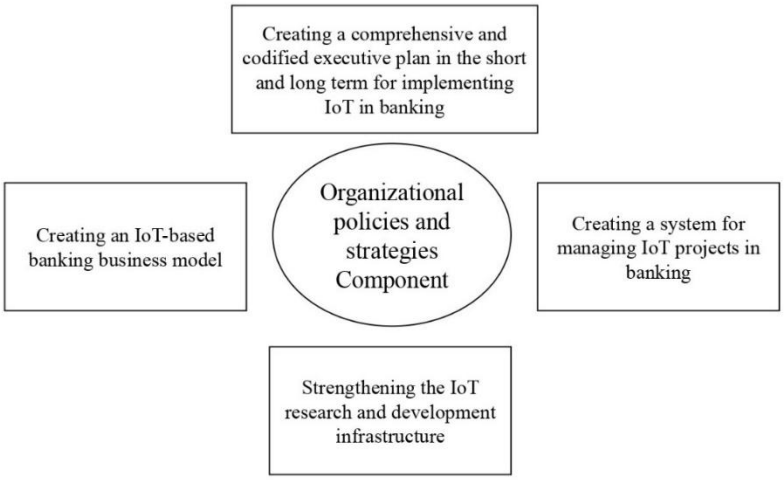

Fig. 8. Indicators of organizational policies and strategies component

4.4.2. Component of rules and regulations (standards, monitoring and evaluation)

In addition to the IoT implementation roadmap, for the effectiveness of the policy framework, the role of internal rules and regulations should also be considered by developers and banking managers for IoT implementation, which includes standards, monitoring, and evaluation [48]. As Saxena and Al-Tamimi, [66], point out in their research, the existence of certain rules and standards is one of the organizational barriers to implementing IoT, The banking industry should also adopt rules and standards that, in addition to facilitating the implementation of the IoT, take into account the interests of all stakeholders and pursue organizational goals while maintaining a balance between their interests. Figure 9 shows the indicators of this component.

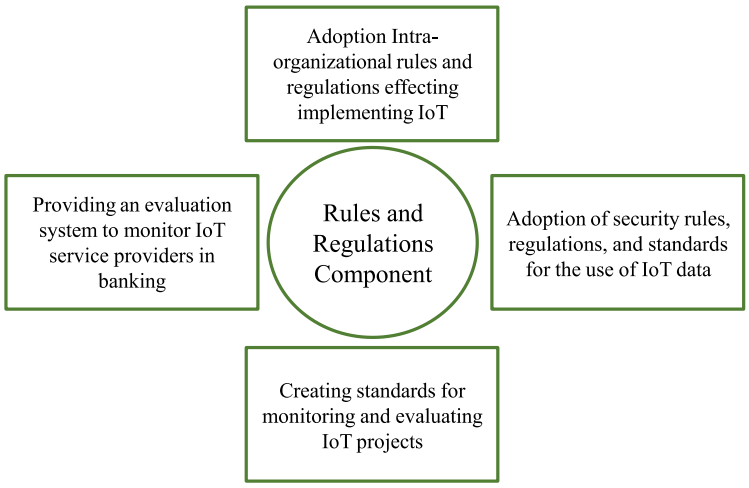

Fig. 9. Indicators of rules and regulations component

4.4.3. Management system component

Several studies consider it important to pay attention to management factors to assess the readiness of the IoT implementation by the organization, including: Careful management and monitor [39,58], Strategic thinking, management commitment, introducing managers to the concepts of ICT and building trust [49], Quality of management methods [59]. Figure 10 illustrates

the indicators of this component. Paying attention to the four indicators mentioned in the figure below by the banking industry can readiness the management system and guide managers to create IoT-based competitive advantages through its implementation. But why is it critical for the management system to be ready to implement IoT? Many managers still have not correctly understood the concepts of IoT, which is due to the lack of training and familiarity of managers with its concepts, which should be achieved through IT managers or at a higher level of government role. One of the reasons can even be the lack of competition and traditional management trends by banking industry managers, especially state-owned banks. These managers can be divided into three categories: 1) Managers who see the IoT as a threat to the organization, 2) Managers who are interested in using IoT in their organization, but are afraid of failure, and 3) managers who fully understand IoT implementation and are not afraid to implement it, but do not know where to start. If there are a strong development team [54] and the appropriate advice to guide managers, then the banking industry can implement IoT with strong managerial backing [48].

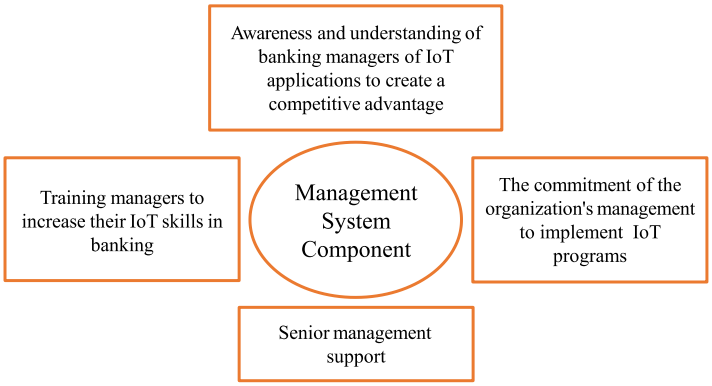

Fig. 10. Indicators of management system component

4.4.4. Component of staff and skills

Most studies have pointed to necessary skills (skilled and expert people) in the IoT ecosystem [6,13,28,40,50,51,54]. Skills can be in the form of IoT-related technical skills, such as data analysis skills [6], academic specialists to collaborate with business [13], and experts with analytical, technical, engineering, etc. skills according to business needs [16,50]. Some studies have used the term staff in addition to skills and experts. Employees can mean office or non-office staff (experts) and even support staff. By preparing their employees to implement IoT and gaining the necessary skills through experts, banks, in addition to preventing staff resistance to using IoT, can familiarize other users, such as customers, with IoT goals through trained staff. Figure 11 depicts the indicators of this component.

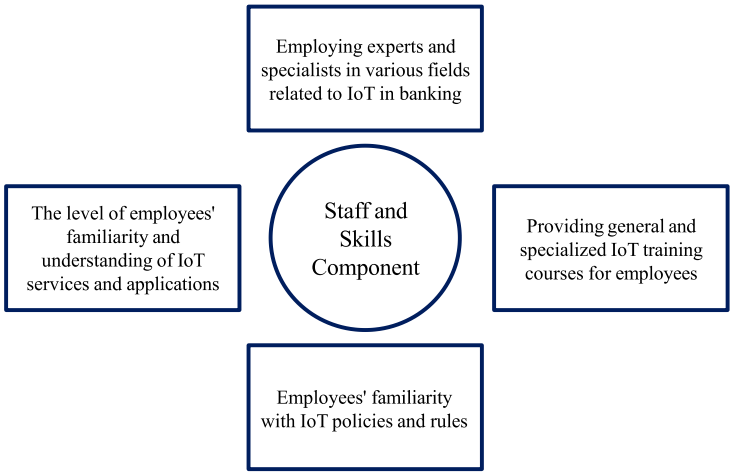

Fig. 11. Indicators of staff and skills component

4.4.5. Financial component

This component refers to significant financial and economic impacts on IoT implementation, which can include the amount of budget allocation, the amount of investment in IoT infrastructure and projects, and financial support. While IoT adoption in banking offers numerous opportunities, it is essential to distinguish between authentic value creation and speculative hype. Lessons from AI's integration into financial markets provide a cautionary tale for evaluating IoT's true impact on banking. Figure 12 illustrates the indicators of this component.

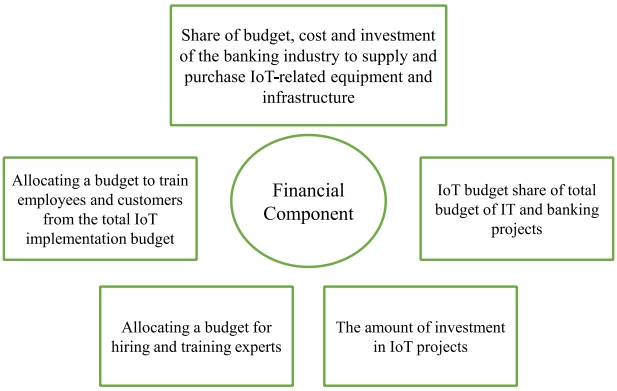

Fig. 12. Indicators of the financial component

4.5. Dimension of customers and training

In two dimensions, organizational and environmental factors, the role of IoT policymakers and developers in customers and education was somewhat mentioned. Most studies have considered the role of the customer and training as an effective factor in implementing IoT in environmental and organizational factors [41]. These studies have directly addressed the end user, i.e., customers, see Table 4. For example, in cooperation with the banking industry, the government should first familiarize its target community (End-users) with IoT-based services and how to use devices, platforms, and applications by holding courses and providing free multimedia training packages. Even according to Baller et al. [59], The amount of customer revenue to use these services should be

considered by businesses, and they should evaluate the affordability of their users, especially customers, whether they can afford to use these services or not. Then implement IoT-based projects. Figure 13 shows the indicators of this component.

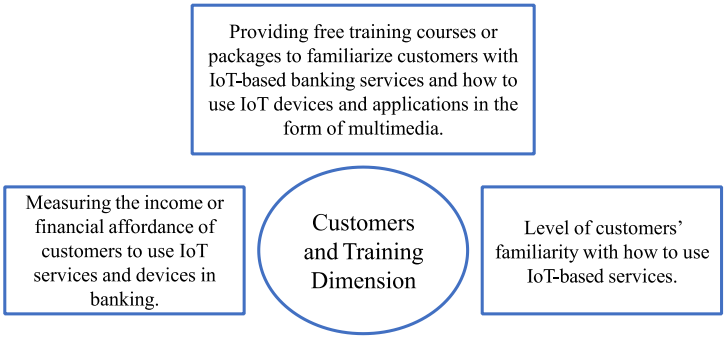

Fig. 13. Indicators of customers and training dimension

4.6. Supply infrastructure dimension

Various studies have examined the importance of this dimension with terms such as suppliers, providers, stakeholders, aid agencies, funding agencies, and the partnership system. See Table 4. In the IoT ecosystem, hard and soft infrastructures are the foundation of IoT (stems and roots), but these stems and roots need nourishment and energy. A coordinated value chain can meet these needs. In the IoT value chain, supply infrastructures play a role in supplying this feed and energy [41]. The table 4 shows the importance of this dimension in the research.

Table 6

The importance of supply infrastructure dimension in the research

Role of supply infrastructures	Research
Domestic companies such as mobile operators and companies active in the field of IT and ICT, Cooperation, and participation of foreign companies	[13]
Stakeholders such as service providers, manufacturing companies, purchasing companies, and mobile operators	[2]
Investment of IT companies	[28]
Cooperation between companies and resource allocation organizations	[50]
Cooperation and communication between stakeholders	[54]
Relevant market stakeholder and supplier interventions	[53]
Competition and cooperation between suppliers	[10,59]
Cooperation of service providers	[12]

As discussed in the section on the environmental dimension of "cooperation and partnership with international companies," this cooperation and partnership is closely related to the supply infrastructures dimension. Service providers may be the public sector, the private sector, or a combination of both. And cooperation between them to provide resources and infrastructure is based on domestic and foreign activities [86]. An example of this collaboration that businesses and IoT project developers should consider is working with mobile operators and Internet service providers. Because they play an important role in communication and network infrastructures. This system of cooperation requires a comprehensive and multilateral system of partnership between

businesses, stakeholders, suppliers, government, and especially the banking industry. The banking industry needs stakeholder cooperation and collaboration to provide IoT services and infrastructure. Even this partnership will create new businesses and technological business models in the banking industry. Figure 14 shows the indicators of this dimension.

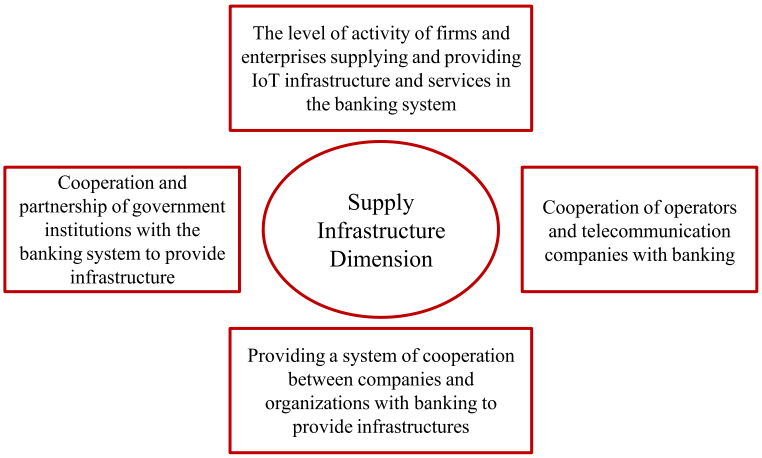

Fig. 14. Indicators of supply infrastructure dimension

4.7. Security and privacy dimension

Security and privacy are among the most important challenges in the IoT ecosystem, and scientific and research perspectives seek to solve related problems and issues. Table (5) shows the importance of this dimension in research. Also, according to Table (1), some studies consider security and privacy as part of the IoT ecosystem. Miorandi et al. [14] refer to the security of IoT data when transferring data from the physical layer to the database and managing it through security and privacy mechanisms with an appropriate security architecture. Wang et al. [33] consider high security and privacy from the beginning of receiving data from the IoT physical layer to displaying and configuring data through web pages. Benias and Markopoulos [57] consider the security of data and information from objects and machines based on sensors and IoT networks to be one of the challenges of Industry 4.0. In their view, lack of security priority by manufacturers, poor data access practices, lack of secure mechanisms for automatic updating, use of public cloud space, and lack of standards and policies for using user data are the concerns of this challenge. And they believe that businesses should consider providers' security features and capabilities before purchasing IoT-based devices and machines. Singh and Singh (2016) consider data security issues the biggest challenge for IoT-connected devices. Concerns about these challenges include privacy leaks, data transfer from Internet-connected devices to the database, lack of common data access standards, technical concerns about data storage and protection, and legal and social concerns [26]. Kunle et al. [2] consider security challenges, especially cultural and social issues, in terms of privacy and users' perceptions of how companies use their data to affect the development and implementation of IoT. Most studies show that security challenges in the IoT ecosystem and its solutions revolve around three issues: 1) Security in IoT devices and objects (physical layer) to prevent tampering and malicious attacks and unrelated access to devices, networks, and communication protocols. 2) Secure path of data transfer from receiving and transferring data to data analysis "Security of servers and data storage space." and 3) Users' privacy preservation or permission to use IoT data and information. The adoption of IoT in the banking industry brings significant security challenges, including potential DDoS attacks. Big data analytics, as highlighted in recent studies, can quantify and mitigate the financial impact of such

attacks, providing valuable insights for enhancing IoT security measures in banking. Given the above research, the banking industry can overcome the security and privacy challenges associated with IoT implementation by adopting the following solutions:

1) Focus on research areas; 2) Adherence to standards related to the IoT ecosystem in its implementation by stakeholders and developers, especially banking industry policymakers; 3) Provide an appropriate security framework and adopt policies to increase the security of infrastructure and data obtained from the IoT and users' privacy; 4) Use of security mechanisms in the IoT implementation process; 5) Compliance with security standards by IoT infrastructure manufacturers and suppliers. Developers and manufacturers of IoT infrastructure can address security challenges by using IoT-converging technologies such as AI, Big Data, computing paradigms, and Blockchain. With the increasing spread of cyber-attacks and the development of IoT applications in financial and banking services, users' concerns will also increase. Failure to address these challenges and concerns will result in financial and non-financial damages and losses in the banking industry and other stakeholders (Bagheri, Zahedian Nezhad, & Panahi, 2023). For this purpose, this study has considered seven indicators for the security and privacy dimension in the banking industry, which are shown in Figure 15.

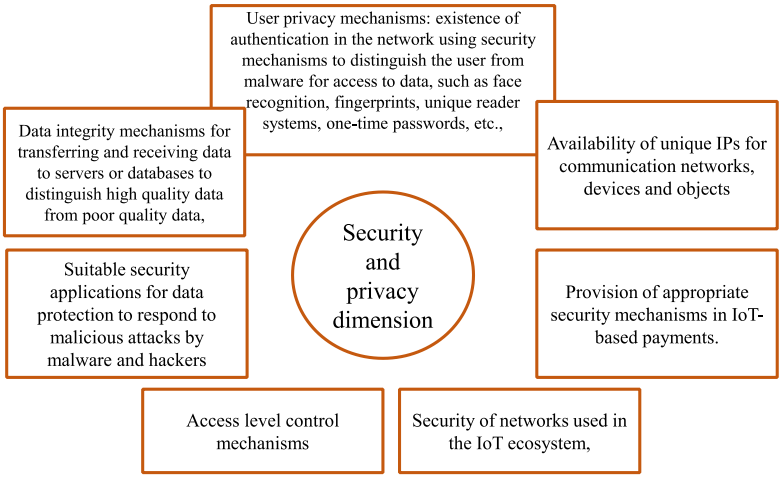

Fig. 15. Indicators of security and privacy dimension

5. Findings of the Fuzzy SWARA Method

Based on the results presented in the table (7), the findings show the fuzzy weights for each dimension of IoT readiness in the banking industry, calculated using the fuzzy SWARA method. The columns represent the fuzzy triangular numbers for each dimension: (representing the upper, middle, and lower bounds, respectively), followed by the crisp weight, and the ranking of each dimension.

Table 7
Ranking dimension by Fuzzy SWARA

No.	Dimension	w_{uj}	w_{mj}	w_{lj}	w_j	ranking
D1	Hard Infrastructure	0.287	0.27	0.245	0.267	1
D2	Soft Infrastructure	0.205	0.2	0.178	0.194	2
D3	Supply Chain Infrastructure	0.173	0.167	0.145	0.162	3
D4	Organizational Factors	0.111	0.105	0.092	0.103	4
D5	Environmental Factors	0.099	0.089	0.075	0.088	5

D6	Customers and Training	0.09	0.087	0.07	0.082	6
D7	Security and Privacy	0.065	0.062	0.05	0.059	7

The results of the fuzzy SWARA method reveal the relative importance of various dimensions for IoT readiness in the banking sector, providing a clear hierarchy based on their calculated weights and rankings. Hard infrastructure emerges as the most critical factor with a weight of 0.267, indicating that robust physical infrastructure, such as hardware, networks, and communication systems, is foundational for supporting IoT deployment in the banking industry. Following closely, soft infrastructure holds a weight of 0.194, emphasizing the importance of organizational readiness, skilled human resources, policies, and internal capabilities that enable the smooth adoption of IoT technologies.

Supply chain infrastructure, with a weight of 0.162, ranks third, highlighting the essential role of efficient logistical systems and the availability of necessary resources in ensuring successful IoT implementation. Organizational factors, which include internal policies, management support, and strategic alignment, come fourth with a weight of 0.103. While these factors are important, they are considered secondary to the infrastructure-related dimensions in ensuring IoT readiness.

Environmental factors, such as regulations are ranked fifth with a weight of 0.088, suggesting that while these external influences affect IoT implementation, they are less significant than the internal infrastructure and organizational aspects. Customers and training, with a weight of 0.082, follow next, indicating the importance of ensuring customer readiness and providing adequate training programs, although this dimension is less critical than infrastructure and organizational factors.

Finally, security and privacy are ranked the lowest with a weight of 0.059. While essential for the integrity and trustworthiness of IoT systems, security and privacy concerns are considered less immediate compared to the need for a strong infrastructure and organizational foundation for IoT adoption.

In conclusion, the findings from the fuzzy SWARA method prioritize hard and soft infrastructure as the most crucial enablers of IoT readiness, while also highlighting the importance of efficient supply chain infrastructure and strong organizational factors. Although security and privacy are vital, they are considered secondary in the early stages of IoT implementation. These insights offer valuable guidance for decision-makers in the banking industry, helping them focus on the most important dimensions to ensure successful IoT integration.

6. Discussion

The IoT offers significant benefits for the banking industry, making proper planning essential to harness its potential at both micro and macro levels. Assessing the readiness of the banking sector for IoT implementation is crucial, involving an evaluation of technical, environmental, and organizational factors. This study assesses IoT readiness by reviewing scientific literature and documents, categorizing enablers into seven dimensions, eight components, and 68 indicators. Validation of the model through a questionnaire revealed that most enablers met the criteria, with only five indicators not validated. These dimensions include ‘Soft Infrastructure,’ ‘Hard Infrastructure,’ ‘Environmental Factors,’ ‘Organizational Factors,’ ‘Customers and Training,’ ‘Supply Infrastructure,’ and ‘Security and Privacy.’

To assess readiness, the banking industry should consider these dimensions. The hard and soft infrastructure relate to ICT and IoT-specific systems, while the environmental dimension covers

cultural, societal, governmental, and legal factors. The organizational dimension includes internal components like strategies, management, staff, and finances. The "Customers and Training" dimension addresses customer skills, training, and revenue. The "Supply Infrastructure" involves actors and stakeholders in the IoT ecosystem, and the "Security and Privacy" dimension deals with security concerns in banking. Effective IoT implementation requires strong ICT infrastructure, including hardware, software, networks, and data analytics, with critical factors like connected object adoption, internet quality, bandwidth, and secure networks. Government, service providers, and startups must collaborate, particularly in developing countries, to enhance ICT infrastructure. The government should enhance ICT infrastructure and promote competition among mobile operators. Technical service providers can supply platforms, operating systems, and IoT-based banking systems like POSs and ATMs.

The IoT ecosystem requires cooperation across businesses, industries, and stakeholders to establish business models such as B2C, B2B, B2G, and G2G. Banks must collaborate with governments and service providers to ensure quality communication and internet services for IoT readiness. Beyond infrastructure, fostering a culture of IoT implementation is essential, considering environmental, organizational, managerial, and societal factors like user trust, interest, literacy, and age. Banks should assess customers' readiness for IoT services, providing training to enhance their familiarity and financial capacity. Government policies and legal frameworks are vital for IoT implementation, addressing cooperation, supervision, and IoT-based financial service regulations, as well as privacy protection.

Organizational factors are key to IoT implementation. Managers must understand IoT's benefits through research and case studies. Senior managers should be aware of IoT's progress, and training is necessary for commitment. Important organizational factors include revising IoT regulations, adopting operational standards, and monitoring service providers' compliance. Clear strategies with defined goals and timelines, along with skilled teams in various fields, are essential. Employees should understand IoT's benefits and policies to reduce resistance and guide customer engagement.

Security and privacy are primary challenges in IoT, particularly in connected objects, communication networks, and computing paradigms. To mitigate risks, banks must adopt security standards and policies within the IoT system. Security requires attention to organizational, managerial, and technical factors. Lastly, managing IoT data requires combining IoT with big data and AI, using advanced algorithms to improve decision support systems (DSS), management information systems (MIS), customer relationship management (CRM), and other systems, creating new business opportunities in banking.

7. Conclusion and Future Directions

The study highlights the significant potential of IoT in transforming the banking industry by leveraging its benefits across various dimensions. Proper planning and thorough assessment of IoT readiness, acceptance, and maturity are critical for successful implementation. This research has identified key enablers across seven dimensions: Soft Infrastructure, Hard Infrastructure, Environmental Factors, Organizational Factors, Customers and Training, Supply Infrastructure, and Security and Privacy. These dimensions encompass a range of technical, organizational, and societal factors that banks must consider. Using the fuzzy SWARA method, the study emphasizes the relative importance of these dimensions. The findings reveal that Hard Infrastructure (0.267) and Soft Infrastructure (0.194) are the most critical enablers for IoT readiness in the banking sector. These factors provide the foundation for IoT deployment, with physical infrastructure (hardware, networks,

communication systems) and organizational readiness (skilled human resources, policies, and internal capabilities) being paramount. Future research should delve into IoT-based banking businesses, the impact of organizational policies and standards, and the convergence of IoT with technologies like big data and cloud computing. Exploring governance frameworks and digital transformation models will further aid in overcoming the challenges of IoT implementation in the banking sector. This comprehensive approach will ensure banks are well-equipped to harness the full potential of IoT, driving sustainable growth and innovation.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was not funded by any grant.

References

[1] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, 22(2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586

[2] Kunle, O. J., Olubunmi, O. A., & Sani, S. (2018). Internet of things prospect in Nigeria: Challenges and solutions. 2017 IEEE 3rd International Conference on Electro-Technology for National Development, NIGERCON 2017, 2018-Janua, 736–745. https://doi.org/10.1109/NIGERCON.2017.8281942

[3] Li, K., Zhang, Y., Huang, Y., Tian, Z., & Sang, Z. (2023). Framework and Capability of Industrial IoT Infrastructure for Smart Manufacturing. Standards, 3(1), 1–18. https://doi.org/10.3390/standards3010001

[4] Albishi, S., Soh, B., Ullah, A., & Algarni, F. (2017). Challenges and Solutions for Applications and Technologies in the Internet of Things. Procedia Computer Science, 124, 608–614. https://doi.org/10.1016/j.procs.2017.12.196

[5] Roe, M., Spanaki, K., Ioannou, A., Zamani, E. D., & Giannakis, M. (2022). Drivers and challenges of internet of things diffusion in smart stores: A field exploration. Technological Forecasting and Social Change, 178, 121593. https://doi.org/10.1016/j.techfore.2022.121593

[6] Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? Business Horizons, 60(5), 667–676. https://doi.org/10.1016/j.bushor.2017.05.010

[7] heidari, A. A. , Amiri Sardari, Z. , Jamshidi, M. J. , & Salarzahi, H. (2020). Investigating the Effects of Infrastructure and Technology of Infrastructure Ecotourism on the Recruitment of Business Angels in Development of Rural Tourism Industry of Kermanshah Province.

Journal of Entrepreneurship Development, 13(2), 199-216. https://doi:10.22059/jed.2020.300443.653319

[8] Talebi, K. , & Abdoli Mohammadabadi, T. (2013). Growth Factors in Small and Medium Industrial Enterprises Producing Clothing owned by Women Entrepreneurs. Journal of Entrepreneurship Development, 6(2), 75-93. https://doi:10.22059/jed.2013.36260

[9] Shah, S. H., & Yaqoob, I. (2016). A survey: Internet of Things (IOT) technologies, applications and challenges. 2016 4th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2016, 381–385. https://doi.org/10.1109/SEGE.2016.7589556

[10] Shin, D.-I. (2017). An exploratory study of innovation strategies of the internet of things SMEs in South Korea. Asia Pacific Journal of Innovation and Entrepreneurship, 11(2), 171–189. https://doi.org/10.1108/apjie-08-2017-025

[11] Rose, K., Eldridge, S., & Chapin, L. (2015). OCTOBER 2015 THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World. Retrieved from https://www.internetsociety.org/iot

[12] ITU. (2017). Measuring the Information Society Report 2017 Volume 1. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

[13] Kshetri, N. (2017). The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply. Telecommunications Policy, 41(1), 49–67. https://doi.org/10.1016/j.telpol.2016.11.002

[14] Miorandi, D., Sicari, S., Pellegrini, F. De, & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

[15] Sadeghizadeh, H., Markazi, A. H. D., & Shavvalpour, S. (2022). Investigating the relationship between governance and key processes of the Iran IoT innovation system. Sensors, 22(2), 652. https://doi.org/10.3390/s22020652

[16] Samanta, M., Virmani, N., Singh, R. K., Haque, S. N., & Jamshed, M. (2023). Analysis of critical success factors for successful integration of lean six sigma and Industry 4.0 for organizational excellence. The TQM Journal, (ahead-of-print). https://doi.org/10.1108/TQM-07-2022-0215

[17] Osei, B. A., & Kwao-Boateng, E. (2023). Critical Review on Internet of Things (IoT): Evolution and Components Perspectives. https://doi.org/10.5772/intechopen.109283

[18] Nazarian-Jashnabadi, J., Haseli, G., & Tomaskova, H. (2024). Digital transformation for the sustainable development of business intelligence goals. In Decision Support Systems for Sustainable Computing (pp. 169–186). Elsevier. https://doi.org/10.1016/B978-0-443-23597-9.00008-1

[19] Farzad, G., & Roshdieh, N. (2024). The Interplay of Destructive Work Behaviors, Organizational Citizenship Behaviors, and Fiscal Decentralization: Implications for Economic Development in Developing Countries. International Research Journal of Economics and Management Studies IRJEMS, 3(8). https://doi.org/10.56472/25835238/IRJEMS-V3I8P101

[20] Askarzadeh, A., Kanaanitorshizi, M., Tabarhosseini, M., & Amiri, D. (2024). International Diversification and Stock-Price Crash Risk. International Journal of Financial Studies, 12(2), 47. https://doi.org/10.3390/ijfs12020047

[21] Madhumita, G., Das, T., Das, S., Khatri, E., Ravisankar, P., & Hemachandu, P. (2024, April). IoT and AI for Real-Time Customer Behavior Analysis in Digital Banking. In 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) (pp. 198-203). IEEE. https://doi.org/10.1109/ICRTCST61793.2024.10578458

[22] Szczepaniuk, H., & Szczepaniuk, E. K. (2022). Standardization of IoT Ecosystems: Open Challenges, Current Solutions, and Future Directions. In Internet of Things (pp. 23–42). CRC Press.

[23] Chegini, H., Naha, R. K., Mahanti, A., & Thulasiraman, P. (2021). Process automation in an IoT--fog--cloud ecosystem: A survey and taxonomy. IoT, 2(1), 92–118. https://doi.org/10.3390/iot2010006

[24] Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. International Journal of Wireless Information Networks, 27, 340–364. https://doi.org/10.1007/s10776-020-00483-7

[25] Kazenga, T. M., Tuyishimire, J. B., Garba, A. A., Saint, M., & Deen, L. (2017). Development of Internet of Things indicators in Rwanda based on stakeholder analysis. International Conference on Information and Communication Technology Convergence: ICT Convergence Technologies Leading the Fourth Industrial Revolution, ICTC 2017, 2017-Decem, 622–627. https://doi.org/10.1109/ICTC.2017.8191054

[26] Bröring, A., Schmid, S., Schindhelm, C.-K., Khelil, A., Käbisch, S., Kramer, D., … Teniente, E. (2017). Enabling IoT ecosystems through platform interoperability. IEEE Software, 34(1), 54–61. https://doi.org/10.1109/MS.2017.2

[27] Singh, Sachchidanand, & Singh, N. (2016). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015, 1577–1581. https://doi.org/10.1109/ICGCIoT.2015.7380718

[28] Raymond, M., Kamel, S., & Iskander, R. (2015). On the suitability of the work system framework as a methodology for researching IoT implementations in developing countries. 2015 Regional ITS Conference, Los Angeles 2015.

[29] T. R. G., Anandaraj, W., & Sivaranjani, K. N. (2015). Internet of things and India ' s readiness Internet of Things and India ' s readiness. Applied Engineering Research, 10(69), 274–279. Retrieved from www.ripublication.comijaer.htm

[30] Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., … Dallas, U. T. (2019). All One Needs to Know about Fog Computing and Related Edge Computing Paradigms. Journal of Systems Architecture, 289, 289–330. https://doi.org/10.1016/j.sysarc.2019.02.009

[31] Chauhan, R. P. S., Sonker, S. K., Kaur, M., Sharma, C., Singh, R., & Singh, R. (2024, March). Optimizing IoT Threat Mitigation with Artificial Intelligence in Banking: A Multi-Objective Approach. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 296-301). IEEE. https://doi.org/10.1109/ICDT61202.2024.10489615

[32] Singh, Saurabh, Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63, 102364. https://doi.org/10.1016/j.scs.2020.102364

[33] Jayapriya, J., Arulmozhi, M., Jagadeesh, V., Sandhiya, M., & Ali, A. N. (2024, May). Enhancing Bank Locker Security through Multi-Layered Authentication and IoT

Integration. In 2024 IEEE Recent Advances in Intelligent Computational Systems (RAICS) (pp. 1-6). IEEE. https://doi.org/10.1109/RAICS61201.2024.10689894

[34] Wang, X., Qiu, H., & Xie, F. (2018). A survey on the industrial readiness for internet of things. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 2018-Janua, 591–596. https://doi.org/10.1109/UEMCON.2017.8249015

[35] Amiri Sardari, Z., Abdoli Mohamadabadi, T., Nazarian-Jashnabadi, J., Tesoriere, G., & Campisi, T. (2024). Smart Experience and Green Health Tourism: The Moderating Role of Content Marketing. Sustainability, 16(11), 4546. https://doi.org/10.3390/su16114546

[36] Phathela, K., & Henney, A. J. (2024, March). Internet of Things Application in South African Breast Milk Banks. In 2024 Conference on Information Communications Technology and Society (ICTAS) (pp. 139-143). IEEE. https://doi.org/10.1109/ICTAS59620.2024.10507145

[37] Banat, H. F. M., Alotoum, F. J., & Hashem, T. N. (2024, February). Smart Banking Services and Their Impact on the Customers' Intentions to Use Mobile Banking in Commercial Banks: Evidence from UAE. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-7). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532845

[38] Tan, W. C., & Sidhu, M. S. (2022). Review of RFID and IoT integration in supply chain management. Operations Research Perspectives, 100229. https://doi.org/10.1016/j.orp.2022.100229

[39] Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers & Security, 105, 102237. https://doi.org/10.1016/j.cose.2021.102237

[40] Cheryl, B.-K., Ng, B.-K., & Wong, C.-Y. (2021). Governing the progress of internet-of-things: ambivalence in the quest of technology exploitation and user rights protection. Technology in Society, 64, 101463. https://doi.org/10.1016/j.techsoc.2020.101463

[41] Zulkipli, N. H. N., & Wills, G. B. (2021). An exploratory study on readiness framework in IoT forensics. Procedia Computer Science, 179, 966–973. https://doi.org/10.1016/j.procs.2021.01.086

[42] Sulaiman, N., & others. (2021). The internet of things readiness in public organization: Descriptive analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), 2017–2022. http://dx.doi.org/10.17762/turcomat.v12i3.1040

[43] Farahmand, A. A., Radfar, R., Poorebrahimi, A., & Sharifi, M. (2021). Investigating the Factors Affecting the Readiness Level of IoT Technology Acceptance (Case Study: Financial Activists, Stock Exchange, and Financial Institutions). Journal of Advances in Computer Engineering and Technology, 7(2), 103–114. https://sanad.iau.ir/en/Article/789530?FullText=FullText

[44] Sar\i, T., Güle\cs, H. K., & Yi\ugitol, B. (2020). Awareness and readiness of Industry 4.0: The case of Turkish manufacturing industry. Advances in Production Engineering & Management, 15(1), 57–68. https://DOI:10.14743/apem2020.1.349

[45] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102

[46] Shalaginov, A., Iqbal, A., & Olegård, J. (2020). Iot digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications. Edge Computing--EDGE 2020: 4th International Conference, Held as Part of the Services

Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 4, 1–17. https://doi.org/10.1007/978-3-030-59824-2_1

[47] Radenković, M., Bogdanović, Z., Despotović-Zrakić, M., Labus, A., & Lazarević, S. (2020). Assessing consumer readiness for participation in IoT-based demand response business models. Technological Forecasting and Social Change, 150, 119715. http://dx.doi.org/10.1016/j.techfore.2019.119715

[48] Mohammadian, H. D. (2020). IoT-Education technologies as solutions towards SMEs' educational challenges and I4. 0 readiness. 2020 IEEE Global Engineering Education Conference (EDUCON), 1674–1683. https://doi.org/10.1109/EDUCON45650.2020.9125248

[49] Sabri, O., Hakim, T., & Zaila, B. (2020). The role of hofstede dimensions on the readiness of iot implementation case study: Saudi universities. Journal of Theoretical and Applied Information Technology, 98(16), 1–12.

[50] El-Aziz, R., El-Gamal, S., & Ismail, M. (2020). Mediating and moderating factors affecting readiness to IoT applications: the banking sector context. International Journal of Managing Information Technology (IJMIT) Vol, 12. http://dx.doi.org/10.5121/ijmit.2020.12401

[51] Kaba, B. (2019). Identifying an analytical tool to assess the readiness of aid information and communication technology projects. The Electronic Journal of Information Systems in Developing Countries, 85(3), e12072. https://doi.org/10.1002/isd2.12072

[52] Castelo-Branco, I., Cruz-Jesus, F., & Oliveira, T. (2019). Assessing Industry 4.0 readiness in manufacturing: Evidence for the European Union. Computers in Industry, 107, 22–32. https://doi.org/10.1016/j.compind.2019.01.007

[53] Calderon, M., Lopez, G., & Marin, G. (2018). Smartness and technical readiness of Latin American Cities: A critical assessment. IEEE Access, 6, 56839–56850. https://doi.org/10.1109/ACCESS.2018.2864218

[54] GSMA. (2018). The Mobile Economy Middle East and North Africa 2018. In GSMA. Retrieved from https://www.gsmaintelligence.com/research/?file=4341c31bb1650dd595909a6761ffd9f0&download

[55] Sheen, D. P., & Yang, Y. (2018). Assessment of Readiness for Smart Manufacturing and Innovation in Korea. 2018 IEEE Technology and Engineering Management Conference, TEMSCON 2018. https://doi.org/10.1109/TEMSCON.2018.8488424

[56] Anggrahini, D., Kurniati, N., Karningsih, P. D., Parenreng, S. M., & Syahroni, N. (2018). Readiness Assessment Towards Smart Manufacturing System for Tuna Processing Industry in Indonesia. IOP Conference Series: Materials Science and Engineering, 337(1). https://doi.org/10.1088/1757-899X/337/1/012060

[57] Arsenijević, D., Stankovski, S., Ostojić, G., Baranovski, I., & Oros, D. (2018). An Overview of IoT Readiness Assessment Methods. Zbornik Radova 8th International Conference on Information Society and Technology--ICIST, 1, 48–53.

[58] IDC. (2017). Prepare for Billions; The IoT 2020 IT Infrastructure Readiness Indicator. An IDC Thought Leadership White Paper, Sponsored by: Hewlett Packard Enterprise, (June), 1–68. Retrieved from https://www.hpe.com/us/en/resources/solutions/iot-readiness-indicator.html

[59] Benias, N., & Markopoulos, A. P. (2017). A review on the readiness level and cyber-security challenges in Industry 4.0. South-East Europe Design Automation, Computer

Engineering, Computer Networks and Social Media Conference, SEEDA-CECNSM 2017. https://doi.org/10.23919/SEEDA-CECNSM.2017.8088234

[60] Ahmad Zaidi, M. F. (2017). The IoT readiness of SMEs in Malaysia: are they worthwhile for investigation? Retrieved from http://repo.uum.edu.my/22935/

[61] Baller, S., Dutta, S., & Lanvin, B. (2016). The Global Information Technology Report 2016. In S. Baller, S. Dutta, & B. Lanvin (Eds.), Lanthanides Series Determination by Various Analytical Methods. https://doi.org/10.1016/b978-0-12-804704-0.00010-4

[62] Schumacher, A., Erol, S., & Sihn, W. (2016). A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises. Procedia CIRP, 52, 161–166. https://doi.org/10.1016/j.procir.2016.07.040

[63] Dineshreddy, V., & Gangadharan, G. R. (2016). Towards an Internet of Things framework for financial services sector. 2016 3rd International Conference on Recent Advances in Information Technology, RAIT 2016, 177–181. https://doi.org/10.1109/RAIT.2016.7507897

[64] Rimer, S. (2017). An IoT architecture for financial services in developing countries. 2017 IST-Africa Week Conference, IST-Africa 2017. https://doi.org/10.23919/ISTAFRICA.2017.8102345

[65] Del Giudice, M., Campanella, F., & Dezi, L. (2016). The bank of things: An empirical investigation on the profitability of the financial services of the future. Business Process Management Journal, 22(2), 324–340. https://doi.org/10.1108/BPMJ-10-2015-0139

[66] Boumlik, A., & Bahaj, M. (2018). Big data and IoT: A prime opportunity for banking industry. In Lecture Notes in Networks and Systems (Vol. 25, pp. 396–407). https://doi.org/10.1007/978-3-319-69137-4_35

[67] Bataev, A. V., Rodionov, D. G., & Kosonogova, E. S. (2018). Evaluation of efficiency of using bank smart-card in Russian financial institutions. International Conference on Information Networking, 2018-Janua, 589–593. https://doi.org/10.1109/ICOIN.2018.8343187

[68] Saxena, S., & Ali Said Mansour Al-Tamimi, T. (2017). Big data and Internet of Things (IoT) technologies in Omani banks: a case study. Foresight, 19(4), 409–420. https://doi.org/10.1108/FS-03-2017-0010

[69] Schimek, R. S. (2016). IoT Case Studies: Companies Leading the Connected Economy. Retrieved from https://www.aig.com/content/dam/aig/america-canada/us/documents/brochure/iot-case-studies-companies-leading-the-connected-economy-digital-report.pdf

[70] Kitchenham, B. (2004). Procedures for Performing Systematic Reviews | BibSonomy. Software Engineering Group Department of Computer Science Keele University. Retrieved from https://www.bibsonomy.org/bibtex/2e48137ec01b6308876e05ab1ecdf4bc4/wiljami74

[71] Sepahi, T., Shahbazi, M., & Shafiei Roudposhti, M. (2020). Drug distribution system in Iran: A multi method study of defects and solutions. Depiction of Health, 11(4), 324–343. https://doi.org/10.34172/doh.2020.41

[72] Nazarian-Jashnabadi, J., Ronaghi, M., Alimohammadlu, M., & Ebrahimi, A. (2023). The framework of factors affecting the maturity of business intelligence. Business Intelligence Management Studies, 12(46), 1–39. https://doi.org/10.22054/ims.2023.74305.2346

[73] Nezhad, M. Z., Nazarian-Jashnabadi, J., Rezazadeh, J., Mehraeen, M., & Bagheri, R. (2023). Assessing dimensions influencing IoT implementation readiness in industries: A fuzzy DEMATEL and fuzzy AHP analysis. Journal of Soft Computing and Decision Analytics, 1(1), 102–123. https://doi.org/10.31181/jscda11202312

[74] LAWSHE, C. H. (1975). A QUANTITATIVE APPROACH TO CONTENT VALIDITY. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

[75] Rajabpour, E., Hamidianpour, F., Hosseini Eghbal, A., & Setayeshmanesh, P. (2022). Identifying and Analyzing the Importance of Key Factors in Employees' Ethical Behavior by Applying Fuzzy SWARA Approach. Ethical Reflections, 3(2), 69-92. https://dor.isc.ac/dor/20.1001.1.26764180.2022.3.2.4.8

[76] Jashnabadi, J. N., Pooya, A., & Bagheri, R. (2023). Provide a model for budget policy in university-community communication programs with a system dynamics approach (case study: Ferdowsi University of Mashhad). J. Ind. Manag. Perspect, 13(1), 9–39. https://doi.org/10.48308/jimp.13.1.9

[77] Mohamadabadi, T. A., Nazarian-Jashnabadi, J., Daryani, M. A., Al-Rashid, M. A., & Campisi, T. (2024). Factors Affecting Online Customer Experience of Food Delivery Services During Crisis: TISM and Delphi Techniques. Sustainable Futures, 100408. https://doi.org/10.1016/j.sftr.2024.100408

[78] Haseli, G., Sheikh, R., & Sana, S. S. (2020). Base-criterion on multi-criteria decision-making method and its applications. International Journal of Management Science and Engineering Management, 15(2), 79–88. https://doi.org/10.1080/17509653.2019.1633964

[79] Haseli, G., Sheikh, R., Wang, J., Tomaskova, H., & Tirkolaee, E. B. (2021). A novel approach for group decision making based on the best–worst method (G-bwm): Application to supply chain management. Mathematics, 9(16), 1881. https://doi.org/10.3390/math9161881

[80] Haseli, G., & Sheikh, R. (2022). Base criterion method (BCM). In Multiple criteria decision making: Techniques, Analysis and Applications (pp. 17–38). Springer. https://doi.org/10.1007/978-981-16-7414-3_2

[81] Haseli, G., Ranjbarzadeh, R., Hajiaghaei-Keshteli, M., Ghoushchi, S. J., Hasani, A., Deveci, M., & Ding, W. (2023). HECON: Weight assessment of the product loyalty criteria considering the customer decision's halo effect using the convolutional neural networks. Information Sciences, 623, 184–205. https://doi.org/10.1016/j.ins.2022.12.027

[82] Haseli, G., Torkayesh, A. E., Hajiaghaei-Keshteli, M., & Venghaus, S. (2023). Sustainable resilient recycling partner selection for urban waste management: Consolidating perspectives of decision-makers and experts. Applied Soft Computing, 137, 110120. https://doi.org/10.1016/j.asoc.2023.110120

[83] Ahmadirad, Z. (2024). The Banking and Investment in the Future: Unveiling Opportunities and Research Necessities for Long-Term Growth. International Journal of Applied Research in Management, Economics and Accounting, 1(2), 34-41. https://ijmeapub.com/index.php/pub/article/download/7/7

[84] Arjmandi, Hossein and Zhao, Xia, "Social Media Impact on FEMA Funding Programs" (2024). AMCIS 2024 Proceedings. 11. https://aisel.aisnet.org/amcis2024/elevlife/elevlife/11

[85] Roshdieh, N., & Farzad, G. (2024). The effect of fiscal decentralization on foreign direct investment in developing countries: Panel smooth transition regression. International Research Journal of Economics and Management Studies IRJEMS, 3(7). https://doi.org/10.56472/25835238/IRJEMS-V3I7P114

[86] Dokhanian, S., Sodagartojgi, A., Tehranian, K., Ahmadirad, Z., Moghaddam, P. K., & Mohsenibeigzadeh, M. (2024). Exploring the impact of supply chain integration and agility on commodity supply chain performance. World Journal of Advanced Research and Reviews, 22(1), 441-450. https://doi.org/10.30574/wjarr.2024.22.1.1119