Int. J. Nonlinear Anal. Appl. 13 (2022) 2, 1771–1787
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.6316

Providing a secure technology transfer model to assess and manage financial and banking risks based on internet of things

Seyed Saman Karimi[a], Tahmoures Sohrabi[b,*], Amir Bayat Tork[b]

[a]Department of Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

[b]Department of Industrial management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

(Communicated by Majid Eshaghi Gordji)

Abstract

The purpose of this applied research was to provide a Risk Assessment Model for Internet of Thing Based Technology Transfer in the Banking Area, and the Strauss and Corbin method is used to identify the initial model. In the qualitative section, by conducting in-depth interviews with 35 experts in the banking technology industry as well as technology-based banking, the information collected was analyzed in three stages open coding, axial coding, and selective coding. In a small part of the statistical population, experts and managers active in the Iranian banking industry, the sample size according to Morgan's table was 386. The results of structural equations and exploratory analysis showed that all relationships between causal factors and the main phenomenon, interfering factors and the main phenomenon The underlying factors and the main phenomenon, the main phenomenon and the strategy, and finally the relationship between the strategy and the results are evaluated in a high to medium level and in a positive and direct way.

Keywords: technology transfer, internet of things (IoT), risk management, banking systems
2020 MSC: 91B05, 91G45

1 Introduction

Nowadays, the issue of developing the use of information technology at all levels is of great importance. Information technology has been able to have profound effects on various Areas, which have caused a great deal of change in modern working spaces [10]. One of the future revolutions has been in the use of information technology in the form of IoT technologies. In these technologies, using information technology and physical objects, a combination of physical and online worlds is done, which can cause enormous changes in the executive operations of organizations [8]. In this regard, in connection with the Internet of Things, there are executive risks that must be continuously considered by the operators of these systems. Some of the most important risks in implementing IoT are [41]: Authentication, which allows the integration of different IoT devices from different platforms [5]. In this context, the risk of authentication is always difficult, which can face more serious challenges based on the development of technological skills [15]. Access permissions that access to different data sources must always be securely protected and only available to access users

*Corresponding author
Email addresses: saman_karimi@ut.ac.ir (Seyed Saman Karimi), tah.sohrabi@iauctb.ac.ir (Tahmoures Sohrabi), a_bayattork@iauctb.ac.ir (Amir Bayat Tork)

Received: November 2021 *Accepted:* February 2022

[4]. Resource depletion in which IoT systems are constantly exposed to attacks by various individuals and hackers [28]. Cryptography where every day new ways are created to crack these codes. In this context, the technologies transfer to IoT-related requires a clear and standard framework that can reduce risk implementation [9]. Among these, one of the most important methods in the banking area, especially with the development of the use of information technology, is to pay attention to risk and risk management in various accounts and bank financial instruments, which can contribute to a high level of public trust in banks, especially be in the digital age. [36]. In this regard, various types of protection and security methods have been used in modern banks around the world, which are classified from soft to hard methods. Most of the hard methods in the form of IoT can be mentioned, which uses information technology to provide physical and technical protection of internal banking systems, especially physical servers. In this context, the use of these systems has been considered as a challenge for bank managers due to the capabilities of hacking and decoding one-time and multiple-use passwords. In this regard, banks use technology transfer to use IoT systems to increase systems security, which can ultimately lead to proper risk assessment and management in the bank [25]. This issue has received less attention in the field of risk management and risk assessment in banking area, which has created a research gap in this field. Therefore, in this study, an attempt is made to provide a comprehensive model for the transfer of IoT-based technology in banks that can implement the necessary management of banking risk in the field of banking and finance. The main objectives of this study are Providing a Risk Assessment Model for Internet of Thing (IoT) Based Technology Transfer in the Banking area, Identify the components affecting the security of IoT-based technology transfer for monitoring and risk assessment in the banking area, Prioritization of components affecting the security of IoT-based technology transfer for monitoring and risk assessment in the banking area,and Providing solutions to implement a secure IoT-based technology transfer model for monitoring and risk assessment in the banking area.

2 Theoretical foundations

Risk management and its process

Risk management project is one of the major topics in project management which includes planning, organizing, monitoring and controlling all aspects of a project and includes risk identification, measurement, risk response development and risk response control [29]. The ideal of this field of management knowledge to help people for continuously protect themselves, their assets and activities against incidents that have always endangered them in the history of human life [31]. Risk management, like other disciplines of management knowledge and its function, utilizes the knowledge, rules, and principles of specific rules to achieve predictions and predetermined goals. The ideal of this field of management knowledge to help people continuously to protect themselves, their assets and their activities against incidents that have always endangered them in the history of human life. This filed which function has been widely practiced since the early 1960s, is in some respects concomitant with human civilization, In fact, its recrudescence is the re-creation of new ways of organizing old ways [31]. In fact, Risk management is a process through which the conditions (probability) of unexpected damages are controlled and managed [34]. The risk management process can be used as a guide for risk management in organizations. Identifying, understanding and preventing risk are among the main goals of risk management [38]. Risk-taking of financial managers compared to other executives managers in the country's management community, the results of a research study showed that financial managers are 85% less likely to take risks than other executive managers [27]. The variety of economic products also force companies to examine more risks pricing, how to internal investment in the risks (how risks can be invested internally) and the value added of services provided by investment banks. In one of the types of risk management processes, this process is categorized into four components:

Risk identification: It is done in order to identify the amount of uncertainty that an organization faces. For this purpose, For this purpose, accurate knowledge of the organization, The market in which it operates, law, society, the existing political and cultural environment, as well as the accurate development of the concept of strategic and operational goals, includes critical factors of success and threats and opportunities that related to these goal are requisite.

Risk assessment: After recognizing the risks of each organization, the impact of each damage on the entire organization should be examined and needs to be determined; First, what is the probability of each damage occurring, and second, what amounts, if any, and how will these amounts affect the financial structure of the organization [31]. We have two approaches to risk assessment, quantitative approach and qualitative approach.

Risk management: It is a vital activity for many processes along with technological risks, especially Shows items in transfer systems [38]. At this stage, in fact, we seek to reduce the probability and financial effects of risky

consequences [18]. In fact, the risk map and priorities made in the organization are the preconditions for starting organizational risk management. Initially, risk management is performed in order to provide an overview of the risks in the organization and to reflect the risks that should be assessed. In the next stage, risk management provides a perspective to consider reducing probability or financial consequences [7]. Unlike some risks are high-level and risk management in an effort to prevent or transfer and share it, there is another risk that is low-level and the organization is trying to adapt it [7].

Risk monitoring: Organizational risks should always be monitored by the organization to consider all its changes and transformations. In this situation, the identified risk management activities should be updated and adapted to the new conditions [18].

Risk management strategies are basically classified into risk responses in these four groups. Also called risk strategies:

1. Avoidance: In this Here, uncertainty should be removed from the project, that is, the occurrence of risk in the project should be made impossible (reduce the probability of its occurrence to zero). Or the plan can be implemented in another way that eventually achieves the same predetermined goals. As a result, the project is safe from the effects of risk. (Zero risk effect on the project)
2. Transfer: Find another risky person who has more ability to manage risk, someone who is responsible for performing the action.
3. Calming: Reducing the amount of risk in order to make it acceptable to the project or organization by reducing the impact or risk's probability.
4. Accept: These risks must be accepted and responded to either actively through appropriate cost allocation or without doing anything passively.

These four types of strategies are only appropriate in relation to threats, otherwise no manager wants to avoid an opportunity or reduce the impact or possibility of occurrence of an opportunity. Therefore, new strategies are needed to respond to opportunities. It is suggested that these strategies can be derived from threat strategies. This can be done by generalizing the method used for threats [1].

Technology transfer and its process

Technology is defined as a combination of physical products or artifacts, product manufacturing processes, and tools combined with physical products. These factors are not separated and separable, but comprised an integrated network that includes technology [40]. The latest definition provided by Muskus extends the concept of technology; In this definition, technology is "the information needed to obtain the main output products by specific methods of combining or processing selected inputs, which include production processes, corporate internal structure, management and financial methods, It becomes marketing methods or any combination of these. [13]. The concept of technology [21] is defined as "knowledge about how to do things" or "the ability of an organization to provide goods or services ordered by its customers, now and in the future." According to this definition, It can be said that choosing technology is a new way of gaining knowledge; Components and systems that help each company to produce more competitive products and services, and create modern solutions. New technologies can provide opportunities for differentiation and new businesses , as well as the importance of accuracy of technology selection for each company's survival [17]. The purpose of the technology transfer method is a set of defined from the defined activities in which the applicant's engineering technology. According to Rizman, in his extensive research on previous articles, economists often define technology transfer based on the general properties of knowledge, in which focuses on production and design variables. Sociologists tend to link technology transfer to innovation and view technology as a desirable outlet. Anthropologists widely see the technology transfer in terms of cultural change and how it affects these changes. According to the United Nations, technology transfer is to import specific technological factors from developed countries 'to developing countries, To enable these countries to prepare and use new production tools and to expand and develop available tools [12]. It is a set of pre-defined activities during which the required technology is provided to the applicant. [16]. Technology transfer is a multidimensional process of communication involving producers , ideas and facilities consumers [19]. In other words, the technology transfer is a range of formal and informal participatory activities between departments, governmental and private and public areas.

The technology includes two main components: 1) Physical component that contains items such as products, tools, equipment, main maps, methods and processes, and 2) information components on knowledge receiver how to manage, marketing, production, quality control, Reliability, skilled personnel and functional fields [13]. Kumar and colleagues, A more advanced definition proposed by Sahal, sees technology as a "configuration" that relies on a mental definition

but can be attributed to processes and products, with a precise review of technology definition, two main components are recognizable: 1) “Knowledge” or procedure and 2) “doing jobs.” [11].

Technology transfer as a multidimensional process of communication that includes manufacturers and consumers of ideas and facilities [19]. In other words, technology transfer encompasses a range of formal and informal collaborative activities between departments, government research departments, and the private and public sectors.Since the term“ Technology transfer” includes many dimensions, often to explain the process in which ideas and concepts from the laboratory are transferred to the labor market [20]. Technology transfer involves a complex process including the complexity of the technology, the complexity of the interaction between the two parts, the ability of the technology owner to train, and the ability of the recipient to learn [33]. Transfer of knowledge and concept from a developed country to less developed country and transfer of innovative activities to the second-hand user is used [23]. This concept not only focuses on the transfer of technical knowledge or information, but also on the ability of the technology recipient to learn and technology absorption in production functions [29]. Technology Transfer is a manner for developing countries for newer technology, these countries should use technology transfers as a basis for completing their technological abilities. These abilities are not limited to physical equipment but also include science and knowledge and the educational abilities and skills of individuals. In industry area, these abilities include choosing, contributing and absorption, improvement and creation of new technology.

The process of technology transfer has a variety of stages that can be divided into three major parts:

Selection and acquisition of technology: The technologies required by each country are determined based on the national technology planning system, a diagnosis that includes the following considerations: is in line with the goals of macro development planning; Although the technology planning system is a dependent system and subject to national development planning, but in terms of the synergistic characteristics of technology developing programs, they are considered as the supra-axis program of coordination of macro-national developing programs; The set of technologies required by each economic section are determined based on the priorities of the relevant section, so that in the next step, the method of supplying each is determined; Although in the step of determining the technology needs of each economic section, it sets its needs with a specific and partial perspective, but in the setp of selecting technology transfer projects, the above selection is made based on a national and cross-sectoral perspective [32].

Adaptation, application and absorption of technology: The process of adapting and linking imported technology with socio-economic conditions, including investment capacity, human skill level, infrastructure facilities, climatic conditions and economic goals and policies [37]. In general, the following measures should be taken: revising the product design and making the necessary changes, modifications and changes in production methods and construction techniques, adapting the building and facilities to the methods and volume of production, reviewing the required organization and management, and reorganizing, Modify and change the product sample.

Development and dissemination of technology: The process of adaptation, application and absorption of technology will continue when new technology is created using the knowledge transferred and the skills and experience gained. Technology development, like the stages of adaptation to absorption and application, has the following stages: designing the production of new products, making a training sample, pilot production of the product and eliminating its shortcomings, mass production.

Internet of things and properties of automated systems

The Internet of Things is not a single technology, but a concept in which many new objects are connected and activated. These have created many business opportunities and added to the complexity of information technology. Distribution, transportation, logistics, reverse logistics, service environment, etc are areas in which information and “objects” are interconnected to create new business processes or a much more efficient and profitable inventory [11]. The rapid convergence of information and communication technology in three layers of technological innovation is taking place: these three layers include the cloud, data and communications, pipes, networks and devices. The convergence of the global network creates the relationship between human, data, and things. This cloud is a convergence force to connect smart things that understand power and transmit a wide array of data. These conditions are helpful in creating services without this level of connection and analytical intelligence. The use of operating systems to transformed technologies such as “cloud”, “things” and “mobility”. The cloud enables global infrastructure in the new services production and allows anyone able to create content and applications for global users [24]. The Internet of Things has become a “universal concept” and needs a common definition. Given the extensive history and technologies required such as measuring devices, communication subsystems, data collection and initial processing to create object samples and finally provide and provide services, producing an unambiguous definition of “Internet of Things”

is important. And is self-evident [6]. Networks of Things (network of Things) connect objects to each other on a global scale and maintain their online identity. Mobile capability provides connectivity to these global infrastructures anytime and anywhere. As a result, a global network enables access to the objects, users, and consumers available to create business, trade, assist content, produce, and purchase new services, and allows connectivity to these global infrastructures. It is available at any time and from anywhere [6].

Operating systems rely on the power of network effects to allow them to access more objects, and they also become more valuable than other objects and users of existing services. The success of an IoT platform strategy can be determined by the connectivity, attractiveness, and flow of knowledge or information or data. Activation of technologies such as sensor networks, RFID, M2M, mobile internet, semantic data integration, semantic search, IPv6, etc., play an important role in the Internet of Things. User interaction on the Internet of Things can be built on a social network template. For example, users interact with each other through social network paradigms with real-world entities of interest. This combination will lead to interesting and popular applications that are more sophisticated and innovative [11]. An infrastructure needs to provide support for security and privacy practices such as authentication, confidentiality, honesty, integrity and integrity of information, authentication, non-denial and accessibility. Heterogeneity and the need for interoperability between different ICT systems based on infrastructure and resource constraints from IoT devices (eg, nano-sensors) should be considered [3]. Use of soft identities, in which the user's real identity can be used to generate various soft identities for specific applications. Each soft identity can be used for a specific context or application. This soft identity is designed without disclosing unnecessary information that could lead to privacy breaches [26].

The following properties are especially important for Internet of Things systems and need further study:

Self-Adaptation: In many dynamic contexts of the Internet of Things, self-adaptation is an essential attribute and provides communication stations. Services also use them to show timely reactions to constant changes [3].

Self-organization: The Internet of Things systems, objects that are members of a network or are automatically separated from it by nodes (stations) are very conventional. Therefore, the network must be able to reorganize itself in the face of this evolving topology.

Self-optimization: Optimal use of limited resources (memory, bandwidth, processor and most importantly energy) of IoT devices is essential for the stability and longevity of IoT extensions.

Self-configuration: The Internet of Things system should provide remote configuration capabilities so that "self-management" applications automatically configure the necessary parameters based on the needs of applications and users.

Self-protection: The Internet of Things at different levels of security and privacy should make its own settings independently, while the quality of service and the quality of experience and expertise are not affected.

Self-healing: The purpose of this feature is to identify and diagnose problems that have occurred and immediately try to resolve them in an independent manner.

Self-description: Objects and resources (sensors and actuators(Drivers)) must be able to describe their features and capabilities in an expressive way in order to allow them to communicate and interact with other objects. Self-description is a fundamental property for plug and play actions of resources and devices.

Self-knowledge: Self-description along with the characteristics of self-knowledge play an essential role in the successful establishment of the Internet of Things. Devices, Internet of Things services should be dynamically discovered and used by others in an integrated and transparent manner.

Self-power supply: Clean energy generation methods (solar, thermal, vibration, etc.) should be used as a main power source instead of batteries that need to be replaced regularly. This action has a positive effect on the environment.

3 Literature review

Mehdi Faraji 2018 in survey technology transfer risk from the perspective of information technology security in e-banking in the electronic field has stated that information security risk assessment methods over the past two decades have helped us well. They have provided a tool for organizations and governments to use them to protect themselves

against the relevant risks. The challenge simply by extending existing assessment methods to IoT systems that we cannot ignore the new risks posed by such ecosystems. These risks can be related to the high degree of connection available or the connection of digital, physical, cyber and social systems. In the IoT Risk Assessment article by [35] is exploring new ways to assess risk in this area, which takes into account the dynamism and uniqueness of the Internet of Things, while maintaining the accuracy of the best method of risk assessment. In a study by [39], Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective confirms that risk distribution can change with any scenario, country and time. With the increasing popularity of IoT devices, human living environments such as smart homes are developing. This development has a negative effect on IoT users. In particular, IoT devices are installed that are equipped with various sensors. However, real security sites are preparing for threats by gaining a uniform degree of risk. A common example is the degree of operation information. K. Kandasamy et al., 2020 provides a comprehensive analysis of cyber risk assessment frameworks, risk vectors, and risk rating processes in the Internet of Things and states that there are many cybersecurity risk assessment approaches and frameworks used in government and commercial organizations. The development of these frameworks in IoT systems alone does not address the new risks posed by the IoT ecosystem. In this study, the usages of IoT risk assessment framework in the field of finance and health care are discussed with the aim of providing maturity in the IoT risk field. They provided a summary of IoT risk assessment with a risk-scoring system suitable for the IoT field to highlight the quantitative approach. Risk rating for IoT risk vector classifies risks into low, medium or high categories. IoT systems in financial technologies and healthcare as a whole are at high risk. The important point of this study ,introducing a new IoT risk calculation model that calculates the risk effect and risk probability and leads to the risk score. In study about Information Security Monitoring and Management Method Based on Big Data in the Internet of Things Environment by [30]. based on the study of the basic technology of the environmental Internet of Things, combined with the service-oriented technology architecture SOA, J2EE, multi-level system architecture MVC, real-time database and other technologies and project practice experience, summarized and proposed a kind of environmental quality monitoring integrated management platform design and implementation feasibility scheme. this study explains the basic principles of constructing the evaluation index system, and establishes the evaluation index system according to the key influencing factors of enterprise information security level in the environment of big data. AHP fuzzy comprehensive evaluation method is chosen on the basis of analyzing various comprehensive evaluation methods, and the weight of each evaluation index is determined and the comprehensive evaluation model is constructed, and the weight given by scientific computing evaluation system, to enhance the practicability of evaluation system, for the Internet of things environment under the background of big data network information security provides a practical guide.

Research gap

As complexity increases,The pervasiveness and automation of technology systems and the maturation of cyberspace, especially with the Internet of Things, there is a strong argument that we will need new methods to assess risk and build trust. Other studies may have attempted to address the issue of IoT and security, but may not have addressed a theory for selecting a secure IoT-based technology transfer model in banking basins. Once the theory is being developed and tested experimentally, further use of the theory to develop criteria and dimensions for testing the model can be quantitative and provide empirical evidence of the model's greater impact. In this study, the proposed solution includes an IoT risk assessment mechanism that determines the risks based on real threats and combines them with the financial regulations in the banking area that must be observed.

4 Research methodology

This research is exploratory and in terms of purpose, it is an applied research and in terms of method, it is a survey and in terms of the type of communication is exploratory. In order to identify the indicators studied in the research, interview tools are used. Also, in the second stage, a questionnaire tool is used to evaluate the fit of the model. In the third stage, a hierarchical comparative questionnaire is used to rank the identified components. In order to measure and identify the components in drawing a conceptual model of qualitative analysis of interviews, as well as using the opinions of experts and through interviews and note-taking tools, information is collected. Finally, a questionnaire is used to assess the functional status of the study. The data collection tool in this research is data collection slips in library studies and qualitative analysis. In the field section, questionnaire and interview tools are used simultaneously. In this study, the sample size is measured based on Cochran's formula in a limited community. Non-random sampling method is targeted. Also in the experts section is the census sampling method. In this section, 35 experts are presented in the category. According to the hybrid approach, several analytical methods are used to provide a comprehensive

model: Qualitative analysis to identify key indicators affecting technology transfer with MAXQODA, AHP to rank the optimal approaches under risk management banking processes Emphasizing the Internet of Things with Expert Choice, Cronbach's alpha test to evaluate the reliability of research tools with SPSS, CVR to evaluate the validity of research tools with ECXELL and SEM with the aim of analyzing the fit of the final model with AMOS.

Nonlinear structural equation model

The traditional linear structural equation model is typically made up of two parts: the measurement model describing the relationships between the observed and latent variables and the structural model describing the relationships between the latent variables. Given a vector of P observed variables Z_i for the ith individual in a sample of size n and a vector of q latent varibles f_i, the linear structural equation model system can be written:

$$Z_i = \mu + \Lambda f_i + \varepsilon_i, \tag{4.1}$$

$$b_0 + B_0 f_i = \delta_{0i}, \tag{4.2}$$

where in the measurement model, the matrices $\mu(p \times 1)$ and $\Lambda(p \times q)$ contain fixed or *unknown scalars* describing the *linear relation* between the observations Z_i and the common *latent factors* f_i, and ε_i represents the $(p \times 1)$ vector of random measurement error independent of f_i such that $E(\varepsilon_i) = 0$ and $Var(\varepsilon_i) = \Psi$ with fixed and unknown scalars in Ψ; and in the structural model, the matrices $b_0(d \times 1)$ and $B_0(d \times q)$ contain fixed or unknown scalars defining d different additive linear simultaneous structural equations relating the factors to one another plus the $(d \times 1)$ vector of random *equation error* δ_{0i}, where $E(\delta_{0i}) = 0$ and $Var(\delta_{0i}) = \Delta_0$ with fixed and unknown scalars in Δ_0.

The simultaneous linear structural model as written in (4.2) is very general. For many practical research questions which can be addressed by simultaneous structural models, it is useful to model specific variables in terms of the rest of the variables , i.e., it is useful to consider some of the latent variables as endogenous and others as exogenous, where *endogenous variables* are those that are functions of other endogenous and *endogenous variables* . Let $f_i = (\eta_i', \xi_i')'$ where η_i are the d endogenous latent variables and ξ_i are the $q - d$ structural model (4.2) becomes:

$$\eta_i = b + B_{\eta_i} + Y\xi_i + \delta_i, \tag{4.3}$$

where it is assumed the *equation errors* δ_i have $E(\delta_i) = 0$, $Var(\delta_i) = \Delta$ and are independent of the ξ_i as well as independent of ε_i in (4.1), and the matices $b(d \times 1), \mathbf{B}(d \times d), \gamma(d \times (q-d))$, and $\Delta(d \times d)$ are fixed or unknown scalars. The structural model (4.3) is said to be in implicit form, implicit because it has endogenous variables on both sides of the equations, i.e., it is not " solved" for the endogenous variables. it is assumed that the diagonal of B is zero so that no element of η_i is a function of itself. A sufficient condition for solving (4.3) is that $(1 - B)$ is invertible, then (4.3) can be solved for the endogenous variables and written as

$$\eta_i = b^* + \Gamma^* \xi_i + \delta_i^*, \tag{4.4}$$

Where $b^* = (1 - B)^{-1} b, Y^* = (1 - B)^{-1} Y$, and $Var(\delta_i^*) = (1 - B)^{-1} \delta (1 - B)^{-1'}$.
The structural model (4.4) is said to be in reduced form as the η_i now appears only on the left-hand side of the equation. it is important to note the assumption that the equation errors δ_i were additive and independent of the ξ_i inthe implicit form (4.3) results in the equation independent of the η_i.

Given p, q and d, additional restrictions must be placed on $\mu, \Lambda, \Psi, b_0, B_0$, and Δ_0 in (4.1) -(4.2) in prder to make all the unknown parameters identifiable. The assumption that (4.2) can be written in reduced form (4.4) is the typical restriction placed on the structural model.

Additionally, a common restriction placed on the measurement model (4.1) is the errors-in-varriables parmeterization where q of the observed variables are each fixed to be equal to one of the q different latent variables plus measurement error. For a thorough discussion of identifiability in linear structural equation models see, e.g.. Finally, it should be noted that there is no inherent distributional assumptions needed for $\varepsilon_i, \delta_{0i}$, nor f_i at this point of model specification although distributional assumptions may be added eventually to perform estimation.

A mixture SEMs for a $p \times 1$ random vector y_i is defined as follows:

$$f(y_i) = \sum_{k=1}^{K} \pi_k f_k(y_i | \mu_k, \sum_k), \quad i = 1, \cdots, n, \tag{4.5}$$

Where K is the number of components which can be unknown, $\mu_k' s$ are component probabilities which are nonnegative and sum to 1.0, $f_k(y|\mu_k, \sum_k)$ is a multivariate normal density function with an unknown mean vector μ_k and a

covariance matrix $\sum_k$. Conditional on the kth component, suppose that y satisfies the following measurement model:

$$y = \mu_k + \Lambda_k \omega_k + \varepsilon_k, \tag{4.6}$$

Where μ_k is an $p \times 1$ intercept vector, Y_k is a $p \times q$*factor loading matrix*, ω_k is a $q \times 1$ random vector of latent variables, and ε_i is a $p \times 1$ random vector of error measurements with distribution $N(0, \Psi_k)$, which is independent of ω_k, and Ψ_k is a *diagonal matrix*. Let Ψ_k be partitioned into $((\eta_n^T, \xi_k^T)^T$, where η_k is a $q1 \times 1$ vector, ξ_k is a $q2 \times 1$ vector, and $q1 + q2 = q$. The structural equation is defined as

$$\eta_k = B_k \eta_k + \Gamma_k \xi_k + \delta_k, \tag{4.7}$$

where B_k and Y_k are $q1 \times q1$ and $q1 \times q2$ matrices of unknown parameters: and random vectors $\xi_k \Lambda_k$ are independently distributed as $N(0, \Phi_k$ and $N(0, \Phi_{\Lambda k}$, respectively: and Φ_k is a diagonal matrix.
We assume that $B_{0k} = (I_{q1} - B_k)$ is nonsingular and (I_{q1} is independent of any elements in B_k. One specific form of B_k that satisfies this assumption is the lower oe upper triangular matrix.
As the mixture model defined in (4.5) is invariant with respect to *permutation* of labels $k = 1, \cdots, k$, adoption of an unique labeling for *identifiability* is important. Roeder and Wasserman (1997), and Zhu and Lee (2001) proposed to impose theordering $\mu_{1,1} < \cdots < \mu_{k,1}$ for eliminating the lable switching (jumping between the various labeling subspace), where $\mu_{k,1}$ is the first element of the mean vector μ_k. This method works fine if $\mu_{1,1}, \cdots, \mu_{k,1}$ are well separated.
However, if $\mu_{1,1}, \cdots, \mu_{k,1}$ are close to each other, it may not be able to eliminate the label switching, and may introduce incorrect results.
Hence, it is necessary to find a sensible identifiability constraint. In this chapter, the *random permutation* sampler developed by Früwrirth-Schnatter (2001) will be applied for finding the suitable identifiability constraints. See the following sections for more details.
Moreover, for each $k = 1, \cdots, K$ structural parameters in the covariance matrix $\sum_k$ corresponding to the model defined by (4.6) and (4.7) are not identified. A common method in *structural equation modeling* for identifying the model is to fix appropriate elements in A_k, B_k and / or Y_k at preassigned values. The positions of the preassigned values of the fixed elements in these matrices of *regression coefficients* can be chosen on a problem-by-problem basis, as long as each $\sum_k$ is identified. In practice, most manifest variables are usually clear indicators of their corresponding latent variables. This give rather clear prior information to specify the zero values to appropriate elements in these parameter matrices. See the illustrative example in Section 5 for a more concrete example. For clear discussion of the proposed method, we let $\pi = (\pi_1, \cdots, \pi_k)$, and θ be the vector which contains all unknown parameters in the covariance matrices that defines an identified model.

Formulation of hypotheses

In order to cover the various dimensions of the problem, research and identify all variables in order to design the final model, we have examined the main variables. For this purpose, we used the Grounded Theory. In the qualitative part of the present study, after in-depth interviews with experts in the banking technology industry as well as technology-based banking, Data collected during the three stages of open coding, axial coding and finally selective coding was analyzed and finally the results of qualitative research. While combining with the results of the research literature, In the first part, the conceptual model of the research was summarized. Interviewees provided answers in accordance with the In-depth Research Interview Questions framework that In evey session, according to the expertise and experience of the respondent in each Organization, the challenges created by the researcher in each interview as well as the researcher's knowledge of these answers are categorized. In this way, the answers provided were categorized based on their type and content in one of the categories of research and were defined and determined as a criterion for evaluating that category. Finally, according to the content of the answers provided, each of the sub-concepts was placed in a related category. It is noteworthy that in the qualitative research process, based on sampling of managers and experts in the field of banking technology, 35 of these people have been collected during in-depth interviews. The coding process is used to analyze the data collected in Grounded Theory method. Coding represents an operation in which data is shredded, conceptualized, and then reconnected in new ways. In this process, the data is analyzed and conceptualized and finally put together in a new way. Strauss and Corbin (1998) divided the coding process into three stages: open, axial, and selective. These units may be words, phrases, or larger pieces of text, these classification are called categories. After classification, meaningful units of text are organized as categories. Strauss and Corbin have proposed this type of coding as open coding, at which point frequently asked questions to clear up coding ambiguities.

In the open coding stage, all interviews with managers and experts are implemented separately and all sentences related to the main research topics are fully recorded and coded, then The researcher has interpreted each of these

key points and coded these points. It is noteworthy, in order to ensure the correct and appropriate coding of key points of expert opinions, after open coding by the main researcher, another researcher has been asked to re-codify all comments based on the points of view of her expertise. Finally, the final code for each of the key points is selected and these codes are numbered. In the relevant tables, in each line, a key point extracted from the interview is mentioned and a marker is assigned for it, which consists of two parts, the first part represents the key point number and the second part indicates the interview number.

The final table of variables and indicators related to each of them was prepared by experts and managers of the banking industry. Then, based on the pairwise comparison questionnaire, the later components are compared. According to the obtained results, the coefficient of importance of the components are presented as the main effective components.

5 Data analysis

- **Qualitative study**

In the qualitative part of the present study, after conducting in-depth interviews with experts in the banking technology industry as well as technology-based banking, the information collected during the three stages of open coding, axial coding and finally selective coding was analyzed and finally the results of qualitative research. While combining with the results of the research literature, the conceptual model of the research was summarized in the form of the first part.

The analysis process starts with open coding and ideally ends with selective coding. Re-coding A qualitative study is the initial coding of a text after repeated and accurate reading of its materials. Meaningful units are introduced, explained and named [2].

Axial (theoretical) coding Qualitative study, or indeed axial coding (second level of coding), is the name given to the secondary operation in data-based analysis in which the main categories of open data coding are developed and interrelated. [2]. At this stage, all open source code extracted from the first stage, based on the relationship with the main concepts of research are summarized in the form of main axes. The output of this step is the axis code, the corresponding code and the number of iterations. Based on this and according to the axial coding performed on the qualitative study of the research, 42 concepts were identified.

Selective coding Qualitative study The third operation in GT analysis is selective coding. The term “selective” is used for this stage because the analyst clearly selects and focuses on a central aspect of the data as the “core category” [2]. In this stage, the central codes of the previous stage were grouped and the final table of variables and indicators related to each of them was prepared from the perspective of experts and managers of the banking industry. In the table related to the selected coding, the concepts related to each category and the frequency of their repetition are mentioned. Accordingly, 42 identified concepts were classified into 6 categories.

In this section, the summary of the two methods (literature review and qualitative study) in the form of the final research model and all its variables are presented in Table 1

Table 1: Variables of the final research model (combination of two methods of thematic literature and qualitative research)

Row	Variable Title	Corresponding concepts
1	**CASUAL**	Technology Transfer Technology Infrastructure Technology transfer software infrastructure Timely risk identification systems Risk assessment systems Improve alignment processes Open technological systems Information security under subsystems Research and development system Funding required
2	**INTERVENING**	Technology Transfer Technology Infrastructure Hardware technology transfer infrastructure
		Level of knowledge of employees Employee acceptance level Ability to integrate information Effective management processes Obligations of senior managers Project teams Manpower training Effective technology transfer management
		Upstream documents of the Central Bank Support from senior bank executives Existence of required technologies in the banking system Transparency of rules
3	**CONTEXTUAL**	Legal factors Financial support Political factors Economic factors Social support Technology transfer planning
		Organizational change management Design of technology-based processes
4	**STRATEGY**	Creating the right infrastructure Technology selection strategy Technology transfer strategy Technology application strategy
		Effectiveness of technology transfer Technology transfer efficiency
5	**RESULT**	Preparation and acceptance of technology transfer reduction in costs Increase revenues
6	**PHENOMENON**	Object-Oriented technology transfer Technology-Base transfer

- **Confirmatory factor analysis of structural model**
  The following model is the final model of this research, this model has been developed according to the conceptual model and with the support of theoretical foundations, this model is in the state of path coefficients, which is equivalent to the analysis of correlation coefficients. The following model summarizes the path coefficients. The structural equation model shows the path coefficients, factor load, error values, and covariances of the obvious variables in this study.

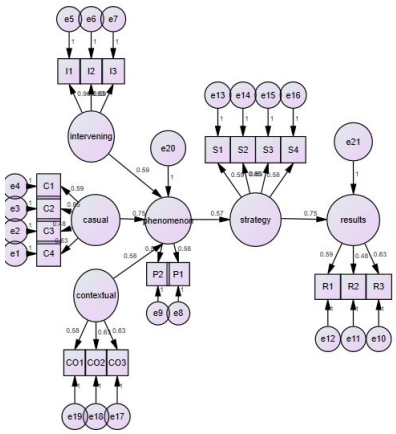

Figure 1: The following model is the final model of this study

As specified in this model, the relationship between latent variables is presented unilaterally. This model also plots the relationship between latent and observed variables. Finally, each of the error coefficients in this model is specified. The values presented above the lines indicate the amount and intensity of the connection.

- **Model fit indicators**
The first criterion for judging the fit is the degree of freedom on the chi-square $\frac{x^2}{df}$, this criterion is used for the one-dimensionality of the structures and its value should be less than 3. $\frac{x^2}{df} = \frac{829.53}{312} = (2.658)$ that this value is less than the value of 3 and the value of $RMSEA = 0.044$, which is less than 0.10. Also, other important fitting indices are listed in the table below, respectively. As can be seen in Table 2, almost all indicators are statistically sufficient, so it can be concluded with great confidence that the researcher has achieved a complete fit for this indicator. And we can confidently analyze the details and graphic relations and test the hypotheses.

Table 2: Selection of important fit indicators of the final drawing model of the research

Indicators	Indicators	Acceptable fit	value	Abbreviation
Absolute fit Index	Covered surface	CMIN/df <3	2.65	CMIN
	Goodness of Fit	GFI> %90	0.98	GFI
	Adjusted Goodness of Fit	AGFI> %90	0.96	AGFI
	Root Mean Square Residual	RMR < 0.08	0.077	RMR
Comparative Fit Index	None Normaed fit index	NNFI> %90	0.96	NNFI
	Normaed fit index	NFI> %90	0.92	NFI
	Comparative Fit Index	CFI> %90	0.93	CFI
	Relative Fit Index	RFI> %90	0.98	RFI
	Incremental Fit Index	IFI> %90	0.98	IFI
ParsimonyNormed Fit	Parsimony Normed Fit Index	PNFI > %90	0.71	PNFI
	Root Mean Square Error ofApproximation	RMSEA< %10	0.044	RMSEA

- **Prioritization of indicators**
In this section, based on the pairwise comparison questionnaire, the components are compared later,and given in tables and diagrams .

Table 3: Pair comparison of intervening components

Transfer management	Readiness	Infrastructure	Components
		1	Infrastructure
	1	2.36	Readiness
1	3.58	4.56	Transfer management
0.085			inconsistency rate

Table 4: Parallel comparison of causal components

provision of budget	Process improvement	Subsystem	Infrastructure	Components
			1	Infrastructure
		1	3.45	Subsystem
	1	4.12	3.65	Process improvement
1	4.2	3.4	4.12	provision of budget
0.09				inconsistency rate

Table 5: Parallel comparison of strategy components

Process	utilization	transfer	Selection	Components
			1	Selection
		1	4.12	transfer
	1	4.2	3.4	utilization
1	4.5	3.6	7.5	Process
0.08				inconsistency rate

Table 6: Parallel comparison of contextual components

PESTLE	Banking management	Banking rules	Components
		1	Banking rules
	1	3.18	Banking management
1	4.56	3.42	PESTLE
0.05			inconsistency rate

Table 7: Parallel comparison of outcome components

Effectiveness	Performance	Readiness	Components
		1	Readiness
	1	4.12	Performance
1	3.5	3.18	Effectiveness
0.088			inconsistency rate

Table 8: Parallel comparison of the components of the central phenomenon

Internet-driven	Technology-driven	Components
	1	Technology-driven
1	4.98	Internet-driven
0.0759		inconsistency rate

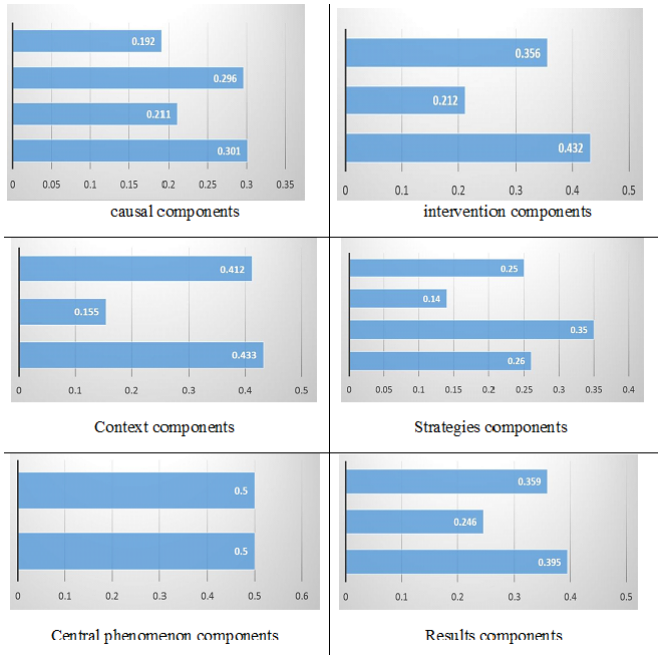

Figure 2: Parallel comparison of components

- **Effective components**

According to the results, components and subcomponents were presented to assess the risk of IoT-based technology transfer, which are presented in the following cases:

Sub-components of causal conditions: infrastructures (technology transfer technology infrastructure, technology transfer software infrastructure), subsystems (timely risk identification systems, risk assessment systems, open technological systems, research and development system, information security in Subsystems), improve alignment processes, provide the required funding.

Interventional sub-components: infrastructure (technology transfer technology infrastructure, technology technology transfer infrastructure, information integration capability), readiness and acceptance (staff knowledge level, staff acceptance level, manpower training), transfer management (processes Effective management, senior management commitments, effective technology transfer management, project teams).

Sub-components of underlying components: laws (upstream documents of the central bank, transparency of laws), Pestle (existence of required technologies in the banking system, legal factors, financial support, political factors, economic factors, social support), extra-bank management (Support of senior banking managers, technology transfer planning).

Results of Sub-components: Effectiveness (technology transfer effectiveness, cost reduction, revenue increase), efficiency (technology transfer efficiency), technology transfer readiness and acceptance.

Sub-component of the main phenomenon: IoT technology transfer, technology transfer.

According to the results, the coefficient of importance of the components of the intervening dimension shows that the components of attention to infrastructure (weight = 0.43), transfer management (weight = 0.35) and readiness (weight = 0.21) have the highest and lowest coefficients of importance, respectively, are dedicated to themselves. Also, in the coefficient of importance of the causal dimensions, it shows that the components of infrastructure (weight = 0.30), process improvement (weight =0.29), subsystem (weight = 0.21) and budgeting [25] have the highest and lowest coefficients of importance, respectively are dedicated to themselves. In the next section, in discussing the coefficient of importance of the next components of the strategies, it shows that the components of transfer (weight = 0.35), selection (weight =0.26), process (weight = 0.25), application (weight = 0.14) are the highest and lowest, respectively Have the highest coefficient of importance. Also, the coefficient of importance of the underlying components shows that the components of banking rules (weight = 0.43), PESTLE (weight = 0.41), banking management (weight = 0.15) have the highest and lowest importance coefficients, respectively . In the significance coefficient of the following components, the results show that the components of readiness (weight = 0.39), effectiveness (weight = 0.35), efficiency (weight = 0.24) have the highest and lowest coefficients of importance, respectively. In the coefficient of importance of the components of the central phenomenon shows that the components of Internet-based (weight = 0.5), technology-oriented (weight = 0.5), respectively, have equal priority.

- **Scientific participation of study (contribution of this study in the development of science)**
The final model of this research, which is in fact its most important output, is shown in Figure 3. As a result of this research, the following model was presented, which is in fact the main innovation of this study, because in this model, the factors affecting the risk transfer of technology transfer are mentioned by mentioning all dimensions.

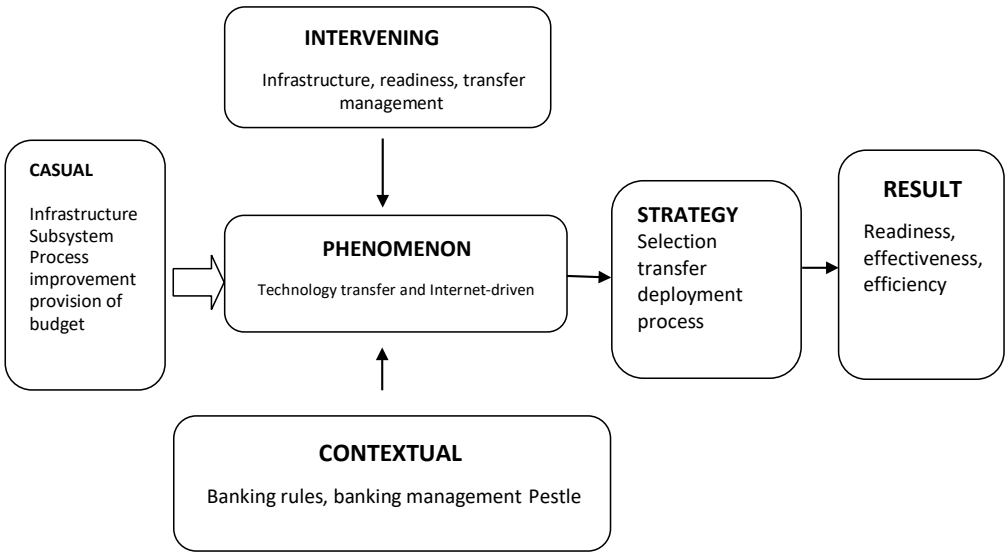

Figure 3: The final research model

6 Conclusion and Recommendations

- **Social implications**

  One of the issues that can be considered in the discussion of risk assessment is the contract in the form of technology transfer technology infrastructure. Therefore, in this section, it is suggested that all the infrastructures required for technology transfer be evaluated in terms of technological systems. In this section, software technology transfer infrastructure has been considered as one of the most important factors in software infrastructure in this regard. Therefore, it is very important to check the level of readiness of the existing software for technology transfer.

  Timely risk identification systems in this study have been considered as one of the causal factors in risk assessment. Therefore, in order to assess any operational risk in the systems, it is necessary to invest in the risk assessment systems so that the important assessment infrastructure and accurate sensors can be used to provide alarm in various directions of project creation and development. Be implemented.

  One of the issues that should be considered in all technology transfer routes is information security under subsystems. To achieve this, all subsystems must be identified and in the next section, information security must be implemented as a subsystem in all sections.

  Continued use of research and development can help organizations to implement information security systems as accurately as possible. In this area, research and development can be effective in identifying risk points.

  One of the issues that should be considered in technology transfer is the knowledge of employees. Technology transfer cannot be implemented without considering specialized knowledge. Therefore, in order to transfer technology correctly in the first step, a level of underlying performance must be considered for this transfer. In this regard, this can be achieved by feasibility study of staff knowledge.

  The level of employee acceptance is very important in technology transfer. In fact, it is by accepting employees that technology can be transferred well. Therefore, before any technology transfer, the level of employee acceptance in this regard should be well evaluated.

  To achieve technology transfer, the ability to integrate information in all sectors must be well implemented. For this issue, in the first step, the executive departments must identify the subsystems, and after identifying these subsystems, using specialized APIs, establish a connection between the departments.

  Commitments of senior managers to implement technology transfer and support these systems can be an effective step in technology transfer.

  The use of specialized project teams in different sectors can have a high impact on technology transfer performance.

  Training of specialized human resources in different parts of technology transfer can reduce the risk of this transfer.

- **Academic implications**

  Risk assessment systems need to be scrutinized in different areas so that a structure can be provided to improve risk assessment .In this regard, the systems should be well analyzed in the risk assessment section and a technology transfer system should be implemented in different sections.

  One of the important strategies in risk assessment is the improvement of aligned systems. In this section, it is necessary to identify all alignment systems in order to integrate the Internet of Things into all existing infrastructures.

  In risk assessment models, appropriate budgeting for projects should be created continuously so that it can finally provide a good picture of the system in the financial departments and financial subsystems of the Internet of Things.

  Considering to effective management processes in different parts of technological systems can be effective in creating coordination between all parts of these systems for technology transfer.

  Timely IoT identification and risk assessment systems are reviewed and updates are always performed.

  Create an environment for exploring IoT-related technological open systems and the security of financial systems.

- **Limitations and future scope**

  Considering to the fact that this research has been conducted in a limited number of banks, it is recommended that this research be reviewed in other public and private banks and compared with the results of this research.

The importance of the role of cultural affairs in accepting technology transfer was examined on a theoretical basis. It is recommended that interested researchers study this variable specifically in the field of technology transfer risk assessment. In order to study more deeply and more accurately identify the different dimensions of the model of this research, each of the components of the model can be studied and measured separately. The focus of this research is on the Internet of Things, and it is suggested that research be conducted in the general field of technology acceptance. A quantitative part of this research was the analysis of the points of view of banking experts and managers. It is recommended to study this issue in future researches from the customers' point of view. The focus of the study is about banks, but smaller-scale models may also be useful for financial institutions to be able to resize to fit the size of any organization in the private or public enterprise.

The main limitation is obtaining unorientated (without direction) answers from banking managers and security experts. For each interview, the researcher kept the interview unscheduled, and bank managers and security experts were not allowed to view the questions before the interview. The questions were asked momentarily during the discussion. Determining the scope made this study focus only on questions without deviating from the topic. Lack of update technology transfer software infrastructure, Difficult access to expert bank staff and managers to answer questions, Access to confidential data, Lack of update technology infrastructure due to political factors and sanctions issues in the country, selected statistical population is limited. Although this study has been inquired from expert bank staff and managers of the bank, but it cannot represent all expert banking managers. Since it is difficult to adapt key factors from all security studies in the field of banking and the Internet of Things, it cannot be assumed that all effective roles in information security in the Internet of Things have been demonstrated in the banking area.

Data availability

The data used to support the results of this study come from PhD dissertation. All the data generated or analyzed during this study are included within this article and dissertation . A request for access to these data and dissertation can be made to the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

We are grateful to the 35 anonymous experts in the category including university professors and banking and government managers and experts in field of banking information technology and government experts and responsible organizations are presented in Iran, for their constructive comments and suggestions on this paper.

References

[1] A. Abdali and A. Naseri, *Expand the risk process to manage opportunities*, Tadbir Month. J. **20** (2003), 12.

[2] K. Abolmaali, *Qualitative research: from theory to practice*, Alam Publishing, Tehran, **402** (1391).

[3] S. Ammirato, F. Sofo, A.M. Felicetti and C. Raso, *A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context*, Eur. J. Innov. Manag. **22** (2019), no. 1, 146–174.

[4] B. Aronson, T. Gonzjlez, K.J. Parker, C. Stöver and A.B. Zampetti, *Synergies for libraries in the least developed countries: The technology bank in pursuit of sustainable development*, 2017.

[5] A. Ashna, E. Golestani, A. Hosseini and J. Zati, *A Study of smart homes and the role of the internet of things and the smart assistant in it*, Fifth Conf. New and Up to Date Achiev. Engin. Sci. New Technol., Rasht, Guilan Industrial Engineering Basij Organization, 2009.

[6] A. Boumlik and M. Bahaj, *Big data and IoT: A prime opportunity for banking industry*, Int. Conf. Adv. Inf. Technol. Serv. Syst., Springer, Cham, April, 2017, p. 396–407.

[7] C. Brindley, *Supply chain risk*, Hampshire, Ashgate Publishing, 2004.

[8] C.S. Choi, J.D. Jeong, J. Han, W.K. Park and I.W. Lee, *Implementation of IoT based PV monitoring system with message queuing telemetry transfer protocol and smart utility network*, Int. Conf. Inf. Commun. Technol. Convergence, IEEE, 2017, p. 1077–1079.

[9] S.E. Crager, *Improving global access to new vaccines: intellectual property, technology transfer, and regulatory pathways*, Amer. J. Public Health **108** (2018), 414–420.

[10] L. Deng, D. Li, X. Yao, D. Cox and H. Wang, *Mobile network intrusion detection for IoT system based on transfer learning algorithm*, Cluster Comput. **22** (2019), 9889—9904.

[11] L. Denis, D.T.K. Kumar, D. Karthikeyan and D.S. Sasipriya, *Offline mobile based OTP technology for enterprise IoT enabled architecture in banking cash logistics and ATM operations*, Int. J. Adv. Res. Engin.Technol. **11** (2020), no. 1, 61–69.

[12] M. Dogson, *The management of technological innovation*, Oxford University Press, 2000.

[13] A. Erumban, *Cross country differences in ICT adoption, a consequence of culture*, J. World Bus. **41** (2006), no. 4, 302–314.

[14] M. Faraji, *Investigation of technology risks from the perspective of IT security in electronic banking in the field of Internet banking*, Int. Conf. New Res. Manag. Econ. Account., 2016.

[15] I. Ganchev, Z. Ji and M. O'Droma, *Designing a low-cost data transfer unit for use in IoT applications*, 8th Int. Cong. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT), IEEE, 2016, p. 85–88.

[16] W. Guo and Sh. Zhang, *Analysis on technology spillover effect of multinational company's technology transfer to the investment of Chinese car industry*, J. Zhengzhou Inst. Aeronautical Ind. Manag. **26** (2008), no. 2, 51–64.

[17] A. Habibi, *Dematel technique training and its applications in management*, Sharif Sci. Res. J. **45** (2012).

[18] J. Hallikas, I. Karvonen, U. Pulkkinen, V.M. Virolainen and M. Tuominen, *Risk Management processes in supplier networks*, Int. J. Prod. Econ. **90** (2004), 47–58.

[19] M. Hosseini and J. Tarokh Mohammad, *Type-2 fuzzy set extension of DEMATEL method combined with perceptual computing for decision making*, J. Ind. Engin. Int. **9** (2013), no. 1, 1–10.

[20] O. Houseman, A. Tiwari and R. Roy, *A methodology for the selection of new technologies in the aviation industry*, Cranfield University, 2004.

[21] A. Jafarnejad, A. Ahmadi and M. Maleki, *Evaluation of lean production using a combined approach of ANP and DEMATEL techniques in fuzzy conditions*, Quart. J. Ind. Manag. Stud. **8** (2011), p. 20.

[22] K. Kandasamy, S. Srinivas, K. Achuthan and V.P. Rangan, *IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process*, EURASIP J. Inf. Secur. **2020** (2020), no. 1, 1–18.

[23] E. Karsak and E.Tolga, *Fuzzy multi-criteria decision-making procedure for evaluating advanced manufacturing system investments*, Int. J. Prod. Econ. **69** (2002), 49–64.

[24] R. Kaur, R.S. Sandhu, A. Gera, T. Kaur and P. Gera, *Intelligent voice bots for digital banking*, Smart Systems and IoT: Innovations in Computing. Springer, Singapore, 2020, p. 401-408.

[25] J. Kirchherr and N. Matthews, *Technology transfer in the hydropower industry: An analysis of Chinese dam developers' undertakings in Europe and Latin America*, Energy Policy **113** (2018), 546–558.

[26] R.S. Lande, S.A. Meshram and P.P. Deshmukh, *Smart banking using IoT,* Int. Conf. Res. Intell. Comput. Engin., IEEE, **4**(2018).

[27] F. Latifi, *Risk and risk-taking*, Tadbir **9** (2000), 20–22.

[28] P.V. Lea, T.A. Manning and U.S. Patent, *Washington, DC: U.S. Patent and Trademark office*, US patent **3** (1967), no. 330, 697.

[29] E. Lee, Y. Park and J. Shin, *Linguistic decision analysis:Steps for solving decision problems under linguistic information*, Fuzzy Sets Syst. **115** (2000), 67–82.

[30] W. Liang, W. Li and L. Feng, *Information security monitoring and management method based on big data in the internet of things environment*, IEEE Access **9** (2021), 39798–39812.

[31] M. Mazloomi, *Risk management*, Account. (1992), 91–92.

[32] L.M. Meade and A. Presley, *Project selection using the analytic network process*, IEEE Trans. Engin. Manag. **49** (2002), 59–66.

[33] L. Ming-Tsang, S. Lin and Y. Tang, *Evaluating RFID adoption by using DEMATEL techniques approach: A case study in Taiwan's Healthcare Industry*, Proc. 12th Asia Pacific Ind. Engin. Manag. Syst. Conf., 2011.

[34] H. Mirzaei, *The need for growth and development of risk management in developing countries*, World Insurance News **59** (2003), 140–144.

[35] J.R.C. Nurse, S. Creese, D. De. Roure, *Security risk assessment in internet of things systems*, IT Prof. **19** (2017), no. 5, 20–26.

[36] D.S. Olawuyi, *From technology transfer to technology absorption: Addressing climate technology gaps in Africa*, J. Energy Nat. Resources Law **361** (2018), 61–84.

[37] M. Ordoobadi Sharon, *Application of ANP methodology in evaluation of advanced technologies*, J. Manufact. Technol. Manag. **23** (2012), no. 2, 229–252.

[38] G.A. Papadakis, *Assessment of requirements on safety management systems in EU regulations for the control of major hazard pipelines*, J. Hazardous Mater. **78** (2000), 63–89.

[39] M. Park, H. Oh and K. Lee, *Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective*, Sensors **19** (2019), no. 9, 2148.

[40] M. Sabeti, *Identifying critical success factors in information systems technology transfer in Iranian organizations*, Manag. Age **4** (2010), 16–17.

[41] S. Stoukatch, F. Dupont, L. Seronveaux, D. Vandormael and M. Kraft, *Additive low temperature 3D printed electronic as enabling technology for IoT application*, IEEE 19th Electron. Packag. Technol. Conf. IEEE, 2017, p. 1–6.