University of Tehran Press

Industrial Management Journal

Online ISSN: 3115 - 7386

Homepage: https://imj.ut.ac.ir

Evaluating Cybersecurity Risks in IoT-Enabled Retail: A Hybrid Pythagorean Fuzzy-SWARA–ARTASI Approach

Mojtaba Norozi [1], **Morteza Piri** ✉ [2], **and Mohamadreza Zahedi** [3]

1. Ph.D. Candidate, Department of Industrial Engineering, Faculty of Management and Industrial Engineering, Malek Ashtar University of Technology, Tehran, Iran. E-mail: mojtabanorozi66@gmail.com
2. Corresponding author, Assistant Prof., Department of Industrial Engineering, Faculty of Management and Industrial Engineering, Malek Ashtar University of Technology, Tehran, Iran. E-mail: piri@mut.ac.ir
3. Associate Prof., Department of Industrial Engineering, Faculty of Management and Industrial Engineering, Malek Ashtar University of Technology, Tehran, Iran. E-mail: Zahedy182@gmail.com

Article Info

Article type:
Research Article

Article history:
Received May10, 2025
Received in revised form August 03, 2025
Accepted November 08, 2025
Available online January 01, 2026

Keywords:
Cybersecurity, Internet Of Things (IoT), retail, SWARA, ARTASI, pythagorean fuzzy sets

ABSTRACT

Objective: This study aims to identify and prioritize cybersecurity risks associated with IoT applications in the retail sector, an area critical to digital transformation and operational resilience. Given the challenges managers face in evaluating threats under uncertainty, the study introduces a novel methodological framework to enhance risk-based decision-making and strategic resource allocation.

Methodology: A hybrid approach combining Pythagorean fuzzy SWARA (PF-SWARA) and an alternative ranking technique based on adaptive standardized intervals (PF-ARTASI) within the FMEA framework is proposed. PF-SWARA is used to weight evaluation criteria, and PF-ARTASI ranks the identified risks. The model is applied to a case study in Iran's retail sector. Sensitivity and comparative analyses are conducted to validate the robustness and effectiveness of the method.

Results: The findings show that "Insecure Firmware/Software and Inadequate Patch Management" is the top cybersecurity risk, followed by "Lack of Standardization and Interoperability Issues" and "Physical Security concerns". The proposed PF-SWARA–ARTASI approach outperforms traditional FMEA and PF-MOORA methods in terms of result consistency, robustness, and practicality under uncertain conditions.

Conclusion: This research makes four contributions: (1) It proposes the first integration of PF-SWARA and PF-ARTASI within FMEA; (2) applies a novel ranking method for risk prioritization; (3) provides an actionable list of prioritized cybersecurity risks in IoT-enabled retail; and (4) validates the model through extensive sensitivity and comparative analysis. The study provides a valuable decision-making tool for IT managers and contributes to the existing literature on fuzzy risk assessment in retail contexts.

Cite this article: Norozi, M., Piri, M., & Zahedi, M., (2026). Evaluating cybersecurity risks in IoT-enabled retail: A hybrid pythagorean Fuzzy-SWARA–ARTASI approach, ***Industrial Management Journal***, 18(1), 22-54. https://doi.org10.22059/imj.2025.400267.1008259

© The Author(s).

Publisher: University of Tehran Press.

DOI: https://doi.org/10.22059/imj.2025.400267.1008259

Introduction

The remarkable advancements in digital technologies have fundamentally reshaped the structure of many industries, with the Internet of Things (IoT) emerging as one of the most influential catalysts of this transformation (Abdullah Sani & Jaafar, 2025). As a cornerstone of the Fourth Industrial Revolution, IoT facilitates intelligent interconnectivity between devices, sensors, and systems, enabling real-time data exchange and significantly improving industrial, service, and consumer operations. By offering capabilities such as predictive analytics, inventory tracking, and waste reduction, IoT significantly contributes to enhancing supply chain productivity and sustainability (Younis et al., 2025). Its global market value surpassed $970 billion in 2022 and is projected to exceed $2.2 trillion by 2028, indicating its pervasive adoption across organizational levels and its role as a foundational infrastructure for innovative business models (Parra-Sánchez, 2025; Abdullah Sani & Jaafar, 2025).

This impact is particularly profound in data-intensive industries such as retail, where operational efficiency and consumer-focused innovation strategies are crucial (Caro & Sadr, 2019). IoT has rapidly disrupted traditional retail paradigms by transforming every stage of the customer journey from pre-purchase to post-sale experiences (Roe et al., 2022). Applications such as dynamic pricing, daily inventory tracking, product traceability, and personalized marketing have enabled retailers to optimize service delivery and deepen engagement with stakeholders (Serral et al., 2020; Kamble et al., 2019). Although Iran's retail sector is still in the early stages of IoT integration, understanding and managing its risks is crucial for strategic decision-making and effective management planning. National initiatives, such as those led by the Iran Telecommunication Research Center, highlight the strategic importance of IoT for economic development (Mohammadzadeh et al., 2018).

However, despite these numerous benefits, the adoption of IoT introduces significant cybersecurity concerns. Poorly secured IoT devices are vulnerable to cyberattacks that may compromise sensitive data, disrupt operations, and pose risks to both enterprises and end-users (Nayak & Swapna, 2023). Cybersecurity has thus become a critical barrier to the diffusion of IoT, as attackers are increasingly motivated by high economic gains and armed with advanced tools (Aslan et al., 2023; Schiller et al., 2022). In IoT-enabled retail environments, where vast volumes of consumer and operational data are continuously exchanged, cybersecurity threats have emerged as significant challenges that can result in substantial financial losses, operational disruptions, and reputational harm. Given the increasing sophistication of cyberattacks and the economic incentives driving them, the structured assessment and prioritization of such risks are indispensable for the successful and secure implementation of IoT solutions in the retail sector (Aslan et al., 2023; Nayak & Swapna, 2023).

To systematically identify and assess cybersecurity risks, various qualitative and quantitative risk assessment models have been utilized. Among them, Failure Mode and Effects Analysis (FMEA) is widely recognized as a structured and systematic risk assessment technique that evaluates risks by focusing on three key dimensions: Severity, Occurrence, and Detection, thereby providing a quantitative basis for risk prioritization and decision-making in complex systems (Gheidar-Kheljani & Roshandel, 2021; Maghami et al., 2024). Although widely used, the RPN index in FMEA has limitations, including the precise values of the RPN determinants not being definitively established. Moreover, the incomplete ranking (characterized by the absence of distinctions in prioritization) and the necessity for uniform weights for the RPN determinants constitute an additional limitation of this conventional scoring method (Altubaishe & Desai, 2023). To address these issues, researchers have increasingly incorporated fuzzy set theory into multi-criteria decision-making (MCDM) frameworks to handle uncertainty better and improve decision accuracy (Behnia et al., 2023; Nazari-Shirkouhi & Zarei Babaarabi, 2025). Pythagorean fuzzy sets (PFS), in particular, offer greater flexibility in representing uncertainty compared to intuitionistic fuzzy sets, and have demonstrated strong potential in complex decision environments (Yager, 2013; Ayyildiz, 2022).

Despite the growing application of fuzzy logic in multi-criteria decision-making (MCDM), a significant gap remains in the literature regarding the evaluation of cybersecurity risks to IoT applications in the retail sector using an integrated Pythagorean fuzzy set-based approach. In particular, the use of the Alternative Ranking Technique based on Adaptive Standardized Intervals (ARTASI), a robust method for ranking alternatives, combined with the Stepwise Weight Assessment Ratio Analysis (SWARA) within a PFS framework, has not yet been explored. To fill this gap, this study proposes a novel hybrid approach that integrates PF-SWARA for weighting criteria and PF-ARTASI for ranking risks, thereby enabling a comprehensive evaluation of cybersecurity threats in retail IoT settings.

The contributions of this study are fourfold:

(a) Proposing a novel FMEA approach integrating SWARA and ARTASI within a Pythagorean fuzzy framework;

(b) Applying PF-ARTASI for effective prioritization of cybersecurity risk factors;

(c) Systematically identifying and ranking key cybersecurity risks in retail IoT applications;

(d) Conducting sensitivity and comparative analyses to validate the robustness and applicability of the proposed method.

The remainder of the paper is structured as follows: Section 2 reviews the relevant literature on IoT, cybersecurity risks in the retail sector, and fuzzy MCDM methods; Section 3 presents the methodological preliminaries and outlines the proposed integrated PF-SWARA-ARTASI technique; Section 4 provides the case study analysis and results; and Section 5 concludes with key findings and implications for management theory and practice.

Literature Background

IoT and the retail sector

The IoT, first introduced by Kevin Ashton in 1999, has become a central component of digital transformation over the past few decades. It serves as a critical tool for optimizing processes, enhancing productivity, and supporting data-driven decision-making across industries (Abdullah Sani & Jaafar, 2025). In academic discourse, IoT is defined in multiple ways. The IoT is a network of interconnected physical objects embedded within digital infrastructures, enabling seamless information exchange and processing. This enhances key organizational capabilities such as flexibility, traceability, and data transparency. More broadly, IoT can be viewed as a service-based architecture that promotes global trade and competitiveness by enriching digital interactions (Younis et al., 2025).

IoT systems integrate sensors and communication technologies that allow real-time data collection, sharing, and analysis (Pino et al., 2024). Over the past two decades, this technology has increasingly replaced traditional systems, offering greater efficiency, cost savings, and improved product quality (Pino et al., 2024; Schiller et al., 2022). Recognized as a general-purpose technology, IoT enables smart devices to function autonomously (Jamme & Connor, 2023), supporting operations across locations and enhancing collaboration (Kamble et al., 2019). IoT-generated data enhances decision-making and customer engagement (Rizvi et al., 2020; Ahmetoglu et al., 2022), enabling firms to stay competitive (Roe et al., 2022), particularly during crises such as the COVID-19 pandemic (Ma et al., 2022). Its applications span diverse sectors, including healthcare (Sadhu et al., 2022), agriculture, transportation, energy (Ahmetoglu et al., 2022), manufacturing (Serral et al., 2020), logistics (Pino et al., 2024), and urban planning (Chanal & Kakkasageri, 2020), underscoring its transformative potential.

The existing literature emphasizes the IoT as a transformative force in the retail industry, enabling real-time customer interaction, personalized shopping, and operational enhancements. Its integration into areas such as dynamic pricing, targeted promotions, inventory tracking, and data analytics leads to increased efficiency and effective decision-making at both operational and strategic levels (Younis et al., 2025). Recognized by the World Economic Forum as a driver of retail transformation, IoT empowers innovations like smart carts, interactive fitting rooms, and

mobile payments, which deliver immersive and customized customer experiences (Roe et al., 2022).

The IoT also supports real-time stock monitoring, logistics optimization, and demand-based store layouts (Hassija et al., 2019). Meanwhile, technologies such as smart shelves and robotic assistants enhance service quality (Roe et al., 2022). Data-driven applications improve pricing, product traceability, and resource allocation (Serral et al., 2020; Kamble et al., 2019). Numerous studies have recently examined the application of IoT in retail operations from various perspectives. Table 1 summarizes the key scholarly contributions to IoT applications in the retail sector, highlighting the implementation benefits, challenges, and managerial implications.

Table1. Review of research findings related to the IoT in the retail sector

No.	Authors	Research Findings
1	De Vass et al. (2018)	IoT capabilities improve internal, customer, and supplier integration, enhancing supply chain and organizational performance.
2	Caro and Sadr (2019)	Highlighted IoT's strategic role in integrating retail channels and improving operations.
3	Kamble et al. (2019)	Found IoT improved food quality; barriers included regulations and poor internet infrastructure.
4	Lorente-Martínez et al. (2020)	Managerial attitudes have a significant impact on the adoption of IoT in small and medium-sized physical retail businesses.
5	Adapa et al. (2020)	IoT retailing created novelty, increasing consumer loyalty and purchase intentions.
6	Serral et al. (2020)	Proposed a maturity model to guide IoT adoption based on expert consensus.
7	Khalil et al. (2020)	Developed an RFID-based system for theft prevention, suitable for scalable retail use.
8	De Vass et al. (2021)	IoT helps supply chains collect data, improving visibility and operational clarity.
9	Park et al. (2021)	Practicality and enjoyment drove Korean consumer acceptance of IoT retail applications.
10	Ma et al (2022)	The IoT helps regain market share, although consumer risk aversion limits profitability.
11	Đurđević et al. (2022)	Beacon-triggered promotions improved shopper attention and influenced purchase behavior.
12	Roe et al. (2022)	IoT enhanced customer experience, but security and privacy risks remain critical.
13	Nayak and Swapna (2023)	Identified IoT security risks; proposed certificateless encryption for data protection.
14	Jamme and Connor (2023)	Intelligent vending machines were adopted early in tight-knit rural French communities.
15	Uddin et al. (2024)	Proposed data protection framework focusing on IT capability and employee training.
16	Argyropoulou et al. (2024)	The IoT capability has a positive impact on firm performance through the mediating roles of supply chain integration and capability in the UK retail sector.
17	Ho et al. (2025)	Uses machine learning and aspect-based sentiment analysis to identify 10 new customer experience aspects, enhancing IoT retail strategies in Vietnam.

While Table 1 highlights the diverse applications and managerial benefits of IoT in retail, it also becomes evident that the deployment of such technologies introduces significant cybersecurity concerns. To date, there has been no systematic identification and quantitative ranking of IoT-related cybersecurity risks in retail environments. Many retailers have encountered vulnerabilities during the implementation process. To address this critical gap, the present study adopts a hybrid methodology to systematically identify and prioritize these risks, as discussed in the following section.

Cybersecurity risk factors faced by IoT applications in the retail sector

For this study, risk is defined as "the probability or threat of damage, injury, liability, loss, or any adverse event caused by internal or external vulnerabilities, which may be mitigated through proactive measures" (Ghadimi et al., 2022). The literature review identified 13 risk factors that retailers must consider when implementing IoT techniques successfully. These factors are illustrated in Table 2.

Table 2. Identified cybersecurity risk factors in the implementation of IoT applications

Symbol	Risk Factor	Risk Description	Supporting Literature
A1	Weaknesses in authentication and authorization in IoT devices	Weak authorization and authentication in IoT devices , such as default credentials, insecure interfaces, and non-scalable access controls ,expose retail systems to cyber threats, particularly in multi-user environments that lack robust identity management.	Akhilesh (2019), Caro and Sadr (2019), Tariq et al. (2023), Kaushik and Dahiya (2018), Sivaselvan et al. (2023)
A2	Device operational disruptions and interruptions	Operational disruptions during IoT device restarts, especially in low-power edge devices, create security gaps that attackers can exploit, targeting weak boot-time protections and draining device energy to cause service interruptions.	Kaushik and Dahiya (2018), Roe et al. (2022), Hassija et al. (2019)
A3	Physical security threats	Easily accessible IoT devices are vulnerable to physical attacks, allowing intruders to tamper with hardware, firmware, or software, turn off power, or introduce malicious nodes, severely compromising cybersecurity in retail environments.	Schiller et al. (2022), Sadhu et al. (2022), Alsheikh et al. (2021), Rizvi et al. (2020)
A4	unauthorized access to the IoT network	Unauthorized access enables attackers to stealthily infiltrate IoT networks, allowing them to steal data and remotely control devices. Phishing attacks further increase risks, making retail IoT environments highly susceptible to cyber exploitation.	Hassija et al. (2019), Nayak and Swapna (2023)
A5	Insecure firmware/software and a lack of patch management	Outdated or unpatched IoT firmware and software leave devices vulnerable to cyberattacks, enabling exploitation through known vulnerabilities or device impersonation. Even updates can introduce risks if not implemented and verified securely.	Akhilesh. (2019), Kaushik and Dahiya (2018), Dejon et al. (2019), Feng et al. (2022)
A6	Data transmission challenge	Continuous data transmission over public channels in IoT networks poses a risk of interception and manipulation. Weak encryption, inconsistent data	Kaur et al. (2023), Kaushik and Dahiya (2018), Akhilesh

		formats, and poor classification expose sensitive information to unauthorized access and cyber threats.	(2019), Sadhu et al. (2022)
A7	Big data and cloud computing issues	Integrating IoT with big data and cloud platforms raises cybersecurity risks, including data replay, unauthorized access, and insecure storage. Diverse systems and devices demand adaptive, up-to-date security to prevent breaches and service disruptions.	Nayak and Swapna (2023), Wazid et al. (2019), Stergiou et al. (2018), Kaushik and Dahiya (2018)
A8	IoT Botnets and Distributed Denial of Service (DDoS)	Due to weak security and constant connectivity, IoT devices are prime targets for botnets used in DDoS attacks. These evolving, hard-to-detect threats overwhelm systems and pose growing cybersecurity challenges.	Abu Al-Haija and Al-Dala'ien (2022), Waqas et al. (2022), Kaushik and Dahiya (2018), Salim et al. (2020), Khalil et al. (2020)
A9	Lack of standardization and interoperability issues	Lack of IoT standardization leads to poor device interoperability, fragmented ecosystems, and weakened security. This complicates threat detection and increases legal and privacy risks, underscoring the urgent need for unified cybersecurity protocols.	Brous et al. (2020), Tariq et al. (2023), Verma et al. (2022), Roe et al. (2022)
A10	Regulatory compliance challenges	Rapid IoT growth outpaces regulations, creating privacy and security gaps. Inconsistent laws and unclear data ownership complicate compliance, increasing cybercrime risks and highlighting the need for updated legal frameworks to ensure secure IoT use.	Verma et al. (2022), Roe et al. (2022), Ahmetoglu et al. (2022)
A11	Social engineering	Social engineering exploits human weaknesses to bypass IoT security, targeting users with limited technical knowledge and expertise. By manipulating individuals rather than systems, attackers gain unauthorized access, making this a highly effective cybersecurity threat.	Ghasemi et al. (2019), Aslan et al. (2023), Okeke and Eiza (2023)
A12	Vulnerable supply chain for IoT components	Dependence on diverse third-party suppliers in IoT supply chains introduces cybersecurity risks. Insufficient oversight and unvetted components create vulnerabilities that can be exploited, impacting the entire retail ecosystem's security.	Akhilesh (2019), Alsheikh et al. (2021), Roe et al. (2022)
A13	Lack of human awareness and skills	Lack of IoT security awareness and skills among users and managers increases vulnerability to cyberattacks. Insufficient training and unsafe practices, such as using unverified third-party apps, create entry points for attackers, thereby heightening risks.	Ani et al. (2019), Sadhu et al. (2022)

FMEA and MCDM methods in a fuzzy environment

FMEA approach

FMEA is a widely applied risk assessment tool that systematically evaluates, prioritizes, and addresses risks in systems, products, and processes before they affect end-users (Altubaishe & Desai, 2023; Janatyan et al., 2025). In this framework, risk evaluation is conducted through three fundamental dimensions: Severity, Occurrence, and Detection, which together form the basis of the Risk Priority Number (RPN) and provide a structured and quantitative mechanism for

comparing and prioritizing risks across complex systems (Rahnamay Bonab & Osgooei, 2025). However, the traditional RPN method faces criticism for assigning equal weight to all three factors and failing to produce fully discriminative risk rankings (Altubaishe & Desai, 2023)

To address these limitations, scholars have integrated Multi-Criteria Decision-Making (MCDM) methods such as SWARA, PIPRECIA, AHP, ANP, and BWM into the FMEA framework, enabling more accurate and dynamic weighting of risk factors (Soltanali & Ramezani, 2023). Additionally, the incorporation of fuzzy set theory helps mitigate subjectivity and vagueness in expert judgments, enhancing decision quality (Nazari-Shirkouhi & Zarei Babaarabi, 2025; Yaftiyan et al., 2025). FMEA has been applied in IoT cybersecurity to identify failure factors and recommend mitigation strategies (Haseeb et al., 2021). Li et al. (2018) integrated fuzzy set theory and gray relational analysis to assess smart city security risks, while Mock et al. (2016) used FMEA for smart building security. In retail and logistics, gray correlation analysis highlighted logistics as a key risk factor. Recent developments involve hybrid FMEA models using fuzzy logic and MCDM methods. For instance, DEA-enhanced FMEA improved the risk ranking of the RFID system (Chnina & Daneshvar, 2024), while other studies employed AHP, PROMETHEE, and fuzzy numbers to refine prioritization (Altubaishe & Desai, 2023). Further enhancements include applications in aerospace, innovative products, and IT systems (Tian et al., 2023). Despite these advancements, comprehensive FMEA frameworks tailored specifically for IoT cybersecurity in retail remain limited.

SWARA applications

As an MCDM technique, the SWARA method is widely employed to derive the weights of subjective criteria based on experts' ordered importance judgments (Amiri et al., 2018; Kardani Malekinezhad et al., 2025). It is direct and straightforward, requiring fewer complex comparisons and less effort from decision-makers (DMs) (Alkan, 2024). The SWARA method simplifies decision-making by determining the weight of criteria without requiring extensive evaluations (Sarvari et al., 2024). DMs play a key role in adjusting criteria based on current conditions and incorporating the importance ratios into the weighting process (Ghiaci & Ghoushchi, 2023). Its integration into other MCDM methods enhances its effectiveness, requiring fewer pairwise comparisons than methods like AHP (Balali et al., 2022).

The SWARA method is widely used to give weights to criteria in multiple-criteria decision-making problems. Ghiaci and Ghoushchi (2023) introduced an integrated SWARA-MOORA approach using Pythagorean fuzzy sets to prioritize barriers for IoT-enabled circular economy systems. Görçün et al. (2022) applied a fuzzy SWARA and fuzzy EATWOS methodology to evaluate retail supply chain performance in the face of uncertainties. Furthermore, Maghami et al.

(2024) introduced a hybrid FMEA method that integrates cost and time into RPN calculations, utilizing SF-SWARA and SF-WASPAS to prioritize risks associated with solar grid integration. Alkan (2024) proposed a hybrid MCDM approach with CRITIC, SWARA, and CODAS in an interval-valued picture fuzzy environment. Akram et al. (2024) employed IRNs, SWARA, and ELECTRE I to address uncertainties in expert assessments. Sarvari et al. (2024) employed a three-round Delphi survey, followed by SWARA, to rank human error factors in a non-fuzzy context. Ghoushchi et al. (2023) prioritized clean energy barriers using SWARA and CODAS in an SFS environment. Additionally, Jafarzadeh Ghoushchi et al. (2023) integrated spherical fuzzy SWARA and MARCOS for assessing rural road risk. Alvand et al. (2023) employed a model that integrates FMEA, SWARA, and WASPAS to evaluate construction project risks.

ARTASI technique

ARTASI is a powerful technique for ranking alternatives, enabling more precise comparisons through the adaptive standardization of values and aggregation functions. ARTASI primarily aims to provide a tool for standardizing information, enabling the comparison of various alternatives across multiple and complex criteria (Pamucar et al., 2024). Instead of using the traditional [0, 1] range, ARTASI allows values to be mapped to a custom-defined, standardized range. This adaptive standardization makes this method particularly suited for complex environments where traditional ranking methods may fail to capture the nuances of different criteria. Once the values are standardized, ARTASI compares each alternative with ideal and anti-ideal values (Yalçın et al., 2024; Kara et al., 2024). In combination with other decision support techniques, such as PFS, this method improves ranking precision by addressing the inherent uncertainty in evaluations. A study used the COBRAC-ARTASI method to evaluate Big Data platforms for large-scale enterprises. COBRAC handles pairwise comparisons of ranked criteria, while ARTASI evaluates alternatives through standardized intervals. Findings showed that ease of utilization was the most significant factor, with Microsoft SQL Server as the optimal platform (Pamucar et al., 2024).

Kara et al. (2024) introduced a hybrid Picture Fuzzy CIMAS-ARTASI model for evaluating website performance in human resource management (HRM). This model integrates Multi-Criteria Group Decision-Making (MCGDM) techniques with PFS, aiming to select the most suitable e-recruitment platform for assigning a Chief Information Security Officer (CISO). The CIMAS method calculates expert-determined importance levels for qualitative and quantitative criteria, while ARTASI ranks alternatives based on adaptive standardized intervals. The findings demonstrated the model's robustness, indicating that performance metrics such as website speed and accessibility are crucial in determining the optimal platform for HRM (Kara et al., 2024).

This study offers two primary contributions. Initially, it explores and identifies a comprehensive range of cybersecurity risks affecting IoT applications within the retail sector, with a focus on the Iranian retail sector. Additionally, it provides an in-depth analysis of each identified risk factor to clarify the specific security concerns associated with IoT applications in the retail sector. Second, an adjusted ARTASI is introduced to rank the recognized risk factors. The adjusted ARTASI addresses the challenge of obtaining the global weights of the alternatives related to the traditional ARTASI. The proposed approach addressed some disadvantages of the FMEA method, including the lack of weight assessment for risk factors and the ignoring of uncertainty. The findings of the present study can appropriately inform policymakers and industry practitioners regarding the existing risk.

Materials and Methods

Proposed method

In this study, an integrated framework of FMEA-SWARA-ARTASI is developed under the PF environment to evaluate and prioritize potential risk factors. Regarding the advantages of PFSs applied in this study, the vagueness of the DMs' views is diminished; therefore, the results are more reliable and applicable in real-life cases. This methodology is presented in three main phases. In the first phase, FMEA experts specify the potential risks, considering the severity (S), occurrence (O), and detection (D) of each risk. In the next phase, using the PF-SWARA, weights are assessed for all three factors of the FMEA approach. In the final phase, all the risks specified in the first phase are ranked using the developed PF-ARTASI method, based on the criteria weights obtained in the second phase. The implementation process of the proposed method is shown in Figure 1.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

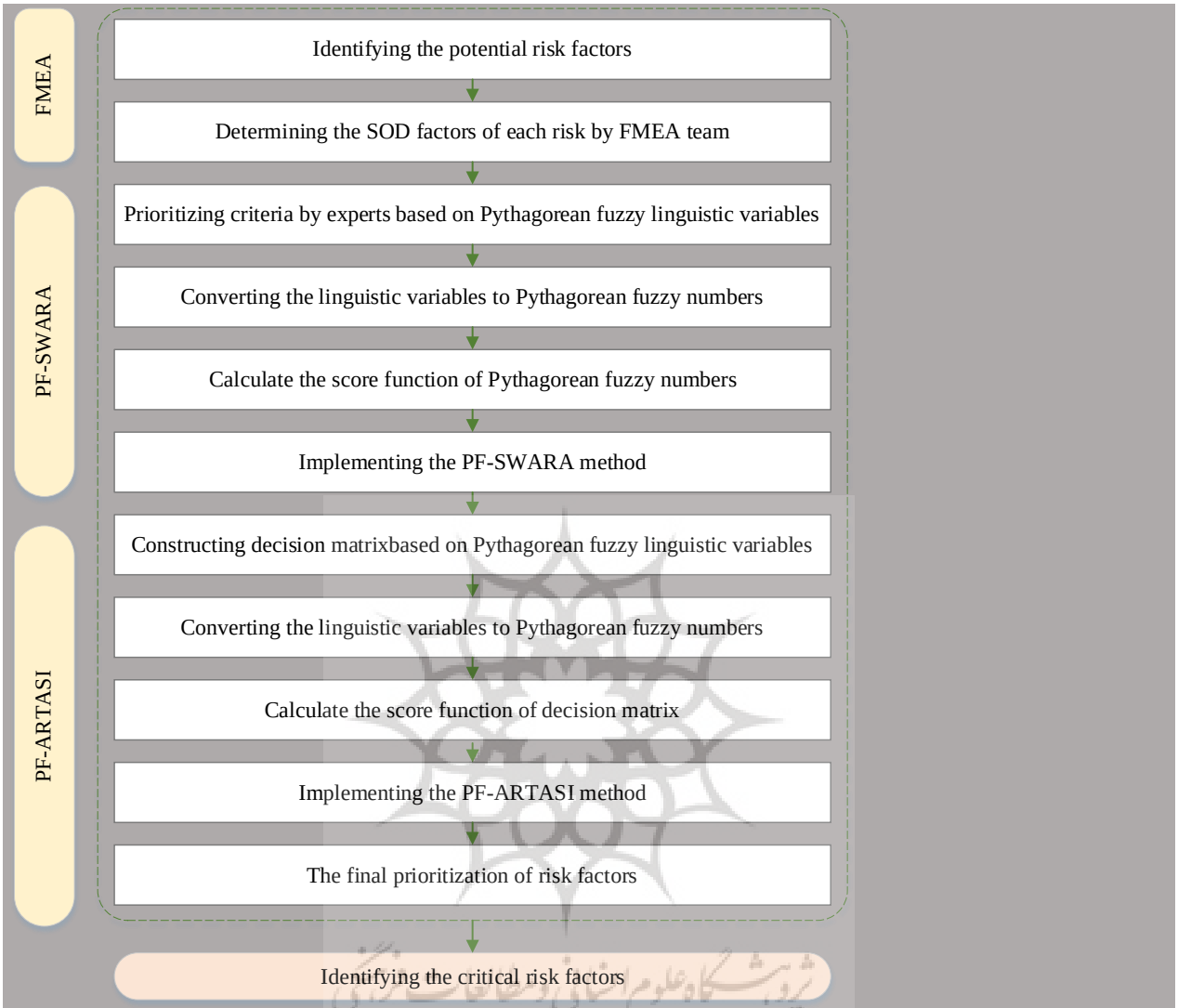

Figure 1. The proposed approach

PF-SWARA

The Stepwise Weight Assessment Ratio Analysis (SWARA) method was initially introduced by Keršulienė et al. (2010) as a structured procedure that enables decision-makers to rank criteria, assess their relative importance, and derive weights systematically and transparently. Subsequent studies have emphasized its practicality and adaptability across various decision-making contexts, particularly due to its straightforward weighting logic (Aghazadeh et al., 2018; Alkan, 2024). The present study aims to enhance the SWARA methodology within the PF-SWARA framework to address certain limitations inherent in the conventional FMEA technique, thereby constituting a more robust methodology for problem resolution. As delineated in Section 2.3, SWARA has been

chosen due to its superior merits compared to alternative weighting methodologies. The procedural steps of the PF-SWARA are briefly given below.

Step 1. Assembling a criterion set by the expert panel

In this step, the expert panel deliberates and scrutinizes the criteria. Decision criteria are delineated as a set. $T = \{T_1.T_2.\ldots.T_n\}$.

Step 2. Developing a decision matrix with PFNs

At this step, the linguistic values (LVs) articulated by the experts will be transmuted into PFNs in accordance with Table 3.

Table 3. LVs and their PFNs

Linguistic values	Pythagorean fuzzy numbers (u, v)
Extremely Low (EL)	(0.15, 0.95)
Very Low (VL)	(0.25, 0.90)
Low (L)	(0.30, 0.85)
Medium Low (ML)	(0.35, 0.75)
Medium (M)	(0.45, 0.65)
Medium High (MH)	(0.60, 0.50)
High (H)	(0.70, 0.35)
Very High (VH)	(0.80, 0.30)

Step 3. Calculation of DEs weight

If A= $\{\mu_A.\nu_A\}$ denotes a PFN; the following formula outlines how to calculate the Kth specialist's weight.

$$\omega_k = \frac{\left(\mu_k^2 + \pi_k^2 \times \left(\frac{\mu_k^2}{\mu_k^2 + v_k^2}\right)\right)}{\sum_{k=1}^{l}\left(\mu_k^2 + \pi_k^2 \times \left(\frac{\mu_k^2}{\mu_k^2 + v_k^2}\right)\right)} \; .k = 1(1)l; \omega_k \geq 0 \; . \sum_{k=1}^{l} \omega_k = 1 \qquad (1)$$

Step 4. Constructing the matrix of aggregated Pythagorean fuzzy decision (APF-D)

The subsequent Equation is employed to amalgamate the DE opinions. The operator is utilized for this Pythagorean fuzzy weighted averaging (PFWA), where $W_{ij}^k = \left[\mu_{ij}^k.\, v_{ij}^k.\, \pi_{ij}^k\right]$ is a Pythagorean number explained by the Kth expert for T_j criteria.

$$z_{ij} = \gamma(\mu_k . v_k) = PFWA_\lambda\left(g_{ij}^{(1)} . g_{ij}^{(2)} . \ldots . g_{ij}^{(l)}\right) = \gamma\left[\sqrt{1 - \prod_{k=1}^{l}(1-\mu_k^2)^{\omega_k}} . \prod_{k=1}^{l}(v_k)^{\omega_k}\right] \quad (2)$$

Step 5. Calculating the weights of the criteria

According to the SWARA method, the expert team initially ranks the specified criteria based on their level of significance in this method, wherein the paramount criterion is prioritized first. Then, other criteria are ranked based on their relative significance. Estimating weights for the criteria through SWARA can be accomplished by following the steps outlined below.

Step 6. SCORE VALUES calculation

It is imperative to compute the SCORE VALUE (Equation 2) to sort the criteria systematically.

Step 7. Sorting criteria

The specified criteria are initially recorded in accordance with their respective score values. The criteria of utmost significance are categorized in the higher categories, while those of lesser significance are classified in the lower categories.

Step 8. Regulating the criteria's proportionate importance (S_j)

The relative importance of the criteria is adjusted in relation to the preceding one.

Step 9. Computing coefficient (K_j)

The coefficient serves as a function reflecting the proportionate significance of criteria, which are computed utilizing the following Equation:

$$K_J = \begin{cases} 1. & j = 1 \\ s_j + 1. & j > 1. \end{cases} \quad (3)$$

Step 10. The calculation of each criterion's initial weight

In this step, each criterion's initial weight is calculated using the Equation below.

$$p_j = \begin{cases} 1. & j = 1 \\ \frac{k_{j-1}}{k_j} & j > 1. \end{cases} \quad (4)$$

Step 11. The final normal weight calculation

Finally, the normalized weight of each criterion is calculated as follows.

$$\omega_j = \frac{p_j}{\sum_{j=1}^{n} p_j} \quad (5)$$

PF-ARTASI

The Alternative Ranking Technique based on Adaptive Standardized Intervals (ARTASI) method was proposed by Pamucar et al. (2024).

Step 1. Decision matrix construction

Let us consider $A = \{A_1 . A_2 . \ldots . A_i . \ldots . A_m\}$ and $C = \{C_1 . C_2 . \ldots . C_j . \ldots . C_n\}$ as the group of alternatives and criteria, respectively. Consider $\Delta = (\varsigma_{ij}) . i = 1(1)m . j = 1(1)n$ a decision matrix presented by the DMs. Therefore, ς_{ij} is the evaluation of alternative A_i about criterion C_j.

Step 2. Converting linguistic variables into PF numbers

The linguistic variables of the decision matrix are transformed into PF numbers, referencing the decision matrix established in the initial step. The decision matrix is then derived using these PF numbers. The conversion is consistent with the data presented in Table 4. Then, crisp values are obtained from the score function.

Table 4. Nine-point scale of Pythagorean fuzzy LVs

Linguistic values	Pythagorean fuzzy numbers
	(u, v)
Extremely low(EL)	(0.10, 0.99)
Very little(VL)	(0.10, 0.97)
little(L)	(0.25, 0.92)
Middle little (ML)	(0.40, 0.87)
Middle (M)	(0.50, 0.80)
Middle high(MH)	(0.60, 0.71)
Big(B)	(0.70, 0.60)
Very tall(VT)	(0.80, 0.44)
Tremendously high (TH)	(1.00, 0.00)

Step 3. Calculating the matrices of absolute maximum and minimum values

It is possible to calculate the absolute maximum and minimum values of a matrix using a crisp decision matrix, as outlined in Equations (6) and (7), respectively.

$$\varsigma_j^{max} = \max_{1\le i\le m}(\varsigma_{ij}) + \left\{\max_{1\le i\le m}(\varsigma_{ij})\right\}^{1/m} \quad (6)$$

$$\varsigma_j^{min} = \min_{1\le i\le m}(\varsigma_{ij}) - \left\{\min_{1\le i\le m}(\varsigma_{ij})\right\}^{1/m} \quad (7)$$

Step 4. Standardizing the initial decision matrix

The standardized decision matrix is calculated using the two steps presented below.

The first-level standardized decision matrix is initially obtained from Equation (8).

$$\phi_{ij} = \frac{\Psi^{(u)} - \Psi^{(l)}}{\varsigma_j^{max} - \varsigma_j^{min}}\varsigma_{ij} + \frac{\varsigma_j^{max}.\Psi^{(l)} - \varsigma_j^{min}.\Psi^{(u)}}{\varsigma_j^{max} - \varsigma_j^{min}} \quad (8)$$

$\Psi^{(u)}$ and $\Psi^{(l)}$ denote the lower and upper limits of the standardized interval.

The second-level standardized decision matrix is estimated by ϕ_{ij} for benefit type criteria and Equation (9) for cost type criteria.

$$\zeta_{ij} = -\phi_{ij} + \max_{1\le i\le m}(\phi_{ij}) + \min_{1\le i\le m}(\phi_{ij}) \quad (9)$$

Step 5. Determining the degree of alternatives' usefulness in terms of the ideal and anti-ideal value

The usefulness degree is determined in terms of the ideal value by expression (10):

$$\vartheta_{ij}^{+} = \frac{\zeta_{ij}}{\max_{1\le i\le m}(\zeta_{ij})}.w_j.\Psi^{(u)} \quad (10)$$

The usefulness degree is determined in terms of the ideal value by expressions (11) and (12).

$$\vartheta_{ij} = \frac{\min_{1\le i\le m}(\zeta_{ij})}{\zeta_{ij}}.w_j.\Psi^{(u)} \quad (11)$$

Where the application of expression (12) defines the degree of utility in relation to the anti-ideal value:

$$\vartheta_{ij}^{-} = -\vartheta_{ij} + \max_{1\le i\le m}(\vartheta_{ij}) + \min_{1\le i\le m}(\vartheta_{ij}) \tag{12}$$

Step 6. Determining the aggregated degrees of the alternatives' utility

The aggregated degrees of the alternatives' utility are determined by expressions (13) and (14).

$$\mathfrak{Q}_i^{+} = \sum_{j=1}^{n} \vartheta_{ij}^{+} \tag{13}$$

$$\mathfrak{Q}_i^{-} = \sum_{j=1}^{n} \vartheta_{ij}^{-} \tag{14}$$

Step 7. Calculating alternatives ranking and final utility functions

Ranking and final utility functions can be determined by the aggregated utility levels. The alternatives' utility functions are estimated by expression (15).

$$\Omega_i = (\mathfrak{Q}_i^{+} + \mathfrak{Q}_i^{-})\{\alpha.f(\mathfrak{Q}_i^{+})^{\varphi} + (1-\alpha).f(\mathfrak{Q}_i^{-})^{\varphi}\}; \varphi \in [1,+\infty);\ \alpha \in [0,1] \tag{15}$$

Where $f(\mathfrak{Q}_i^{+})$ and $f(\mathfrak{Q}_i^{+})$ signify additive functions we obtain as $f(\mathfrak{Q}_i^{+}) = \frac{\mathfrak{Q}_i^{+}}{\mathfrak{Q}_i^{+}+\mathfrak{Q}_i^{-}}$ and $f(\mathfrak{Q}_i^{+}) = \frac{\mathfrak{Q}_i^{-}}{\mathfrak{Q}_i^{+}+\mathfrak{Q}_i^{-}}$.

The alternatives' final ranking is determined by the final utility functions, expression (15), where the alternative should possess the highest value Ω_i.

Results

The findings of the proposed method in this study, which assesses cybersecurity risks associated with IoT applications in the retail sector, are presented in this section. The Pythagorean fuzzy theory is employed due to the uncertainty of the factors. The PFSs corresponding to three factors for each risk, as identified by the FMEA team's observations, are illustrated in Table 5.

Table 5. The decision matrix in the form of Pythagorean fuzzy LVs

	Severity(S)	Occurrence(O)	Detection(D)
A1	M	MH	ML
A2	L	M	M
A3	B	MH	ML
A4	MH	M	M
A5	B	VT	MH
A6	VL	M	MH
A7	VL	L	B
A8	ML	M	ML
A9	B	MH	M
A10	MH	ML	L
A11	VL	L	ML
A12	L	M	ML
A13	B	B	MH

Subsequently, the PF-SWARA approach is utilized to assign weights to the criteria in accordance with the second phase of the proposed method. Within the SWARA method, the involvement of DEs constitutes a crucial element of the criteria weighting procedure. Each DE ascertains the importance of the criteria. The DE then ranks the entire criteria, implicit understanding, and informational resources (Table 6).

Table 6. Pythagorean fuzzy LVs of triple criteria by experts' judgements

DM1		DM2		DM3	
S		S		S	
O	L	O	ML	O	VL
D	VL	D	L	D	ML

Consistent with SWARA and as indicated in Table 4, the verbal suffixes presented in Table 6 are converted into PFNs. The PFWA matrix is established utilizing the weights assigned by the DEs, and three criterion weights are derived employing the SWARA approach, as outlined in Table 7.

Table 7. The weights of the triple criteria calculated by the PF-SWARA method

Criteria	Crisp values	S_i	K_i	P_i	W_i
S			1	1	0.44
O	-0.67	0.67	1.67	0.60	0.26
D	-0.53	-0.14	0.86	0.69	0.30

The prioritization is conducted using the PF-ARTASI method in the third phase of the proposed method, following the results obtained from the initial and second phases. The Pythagorean fuzzy decision matrix presented in Table 5 is transmuted into PFNs in Table 8.

Table 8. Pythagorean fuzzy group assessment matrix

	S		O		D	
	u	v	u	v	u	v
A1	0.50	0.80	0.60	0.71	0.40	0.87
A2	0.25	0.92	0.50	0.80	0.50	0.80
A3	0.70	0.60	0.60	0.71	0.40	0.87
A4	0.60	0.71	0.50	0.80	0.50	0.80
A5	0.70	0.60	0.80	0.44	0.60	0.71
A6	0.10	0.97	0.50	0.80	0.60	0.71
A7	0.10	0.97	0.25	0.92	0.70	0.60
A8	0.40	0.87	0.50	0.80	0.40	0.87
A9	0.70	0.60	0.60	0.71	0.50	0.80
A10	0.60	0.71	0.40	0.87	0.25	0.92
A11	0.10	0.97	0.25	0.92	0.40	0.87
A12	0.25	0.92	0.50	0.80	0.40	0.87
A13	0.70	0.60	0.70	0.60	0.60	0.71

The normalized matrices are calculated according to step 4 and presented in Tables 9 and 10.

Table 9. The first-level normalization matrix

	S	O	D
A1	-47.75	-27.45	-98.91
A2	-90.08	-47.93	-72.89
A3	8.13	-27.45	-98.91
A4	-21.32	-47.93	-72.89
A5	8.13	21.72	-41.96
A6	-105.88	-47.93	-41.96
A7	-105.88	-80.74	-7.49
A8	-69.99	-47.93	-98.91
A9	8.13	-27.45	-72.89
A10	-21.32	-65.16	-122.42
A11	-105.88	-80.74	-98.91
A12	-90.08	-47.93	-98.91
A13	8.13	-4.62	-41.96

Table 10. The second-level normalization matrix

	S	O	D
A1	-47.75	-27.45	-31.01
A2	-90.08	-47.93	-57.03
A3	8.13	-27.45	-31.01
A4	-21.32	-47.93	-57.03
A5	8.13	21.72	-87.96
A6	-105.88	-47.93	-87.96
A7	-105.88	-80.74	-122.43
A8	-69.99	-47.93	-31.01
A9	8.13	-27.45	-57.03
A10	-21.32	-65.16	-7.49
A11	-105.88	-80.74	-31.01
A12	-90.08	-47.93	-31.01
A13	8.13	-4.62	-87.96

The aggregate degree of utility of the alternatives matrix is obtained by expressions (13) and (14) and presented in Table 11.

Table 11. The aggregate degree of the alternative's matrix utility

	$\mathfrak{Q}_i^+$	$\mathfrak{Q}_i^-$
A1	-258.71	-408.29
A2	-484.87	-310.98
A3	40.88	156.90
A4	-116.26	-451.61
A5	155.58	315.70
A6	-539.37	-288.05
A7	-545.16	-268.92
A8	-402.53	-362.67
A9	66.28	196.07
A10	-185.32	-753.29
A11	-634.39	-333.03
A12	-510.27	-350.15
A13	123.91	-12.55

Finally, $\boldsymbol{f}(\mathfrak{Q}_i^+)$, $\boldsymbol{f}(\mathfrak{Q}_i^-)$ and Ω_i are calculated in step 7 as a final step of the proposed method. In this Equation, the values of φ and α are considered 1 and 0.5, respectively. The final score (Ω_i) Moreover, the rank of each risk is obtained based on these three values. As shown in Table 12, we find that A5, which equals 235.646, is prioritized over other risks. A9 and A3, equal to 131.177 and 98.892, hold the second and third priorities, and A11, equal to -483.711, is in the last one. Consequently, specialists can implement preventive and remedial actions based on priorities to mitigate the negative impact of these risks.

Table 12. The ARTASI indices for each risk

	$f(\mathfrak{Q}_i^+)$	$f(\mathfrak{Q}_i^-)$	Ω_i	Rank
A1	0.388	0.61	-333.50	6
A2	0.61	0.39	-397.92	8
A3	0.21	0.79	98.89	3
A4	0.20	0.79	-283.93	5
A5	0.33	0.67	235.64	1
A6	0.65	0.35	-413.71	10
A7	0.67	0.33	-407.04	9
A8	0.53	0.47	-382.60	7
A9	0.25	0.75	131.18	2
A10	0.20	0.80	-469.31	12
A11	0.65	0.34	-483.71	13
A12	0.59	0.41	-430.21	11
A13	1.11	-0.11	55.68	4

Sensitivity and comparative analysis

The sensitivity analysis scenarios have been formulated to evaluate the robustness of the proposed PF-SWARA-ARTASI hybrid model. These scenarios facilitate the examination of the relations between the results derived from the algorithm's implementation across various conditions and the

corresponding research findings. The sensitivity analysis scenarios (SAS) organization is presented below:

Is there any change in alternative rankings if the φ value in the proposed approach is changed?

Is there any change in alternative rankings if the value in the proposed approach is changed?

Table 13 presents the ranking results for different values of φ and α. Based on the results, we find that with the change of φ and α, does not considerably alter the results. Although there are some changes in the priority of risks, the set of critical risks is constant in most scenarios. The change in φ and α does not significantly influence the ranking because A5 (Insecure Firmware/Software and Lack of Patch Management) is identified with high priority in all scenarios. Nonetheless, experts can decide about the values of φ and α based on the characteristics of the data and the specific subject matter.

Table 13. Risks rankings with different φ and α values

	φ=1									
	α = 0.1		α = 0.3		α = 0.5		α = 0.7		α = 0.9	
	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank
A1	-393.33	11	-363.42	8	-333.50	6	-303.58	6	-273.67	7
A2	-328.36	7	-363.14	7	-397.92	8	-432.70	9	-467.48	9
A3	145.30	3	122.10	3	98.89	3	75.69	4	52.48	4
A4	-418.08	12	-351.01	5	-283.93	5	-216.86	5	-149.79	5
A5	299.69	1	267.67	1	235.64	1	203.62	1	171.60	1
A6	-313.19	6	-363.45	9	-413.71	10	-463.98	12	-514.24	11
A7	-296.54	5	-351.79	6	-407.04	9	-462.29	11	-517.53	12
A8	-366.66	10	-374.63	10	-382.60	7	-390.57	8	-398.54	8
A9	183.09	2	157.13	2	131.18	2	105.22	2	79.26	3
A10	-696.50	13	-582.90	13	-469.31	12	-355.71	7	-242.12	6
A11	-363.16	8	-423.44	12	-483.71	13	-543.98	13	-604.26	13
A12	-366.16	9	-398.18	11	-430.21	11	-462.23	10	-494.25	10
A13	1.10	4	28.39	4	55.68	4	82.97	3	110.26	2
	φ =2									
	α = 0.1		α = 0.3		α = 0.5		α = 0.7		α = 0.9	
	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank
A1	-395.89	11	-369.83	5	-341.78	6	-311.23	6	-277.32	6
A2	-332.48	7	-371.78	6	-407.31	8	-439.98	8	-470.38	9
A3	149.41	3	133.17	3	114.65	3	92.49	4	62.98	4
A4	-430.01	12	-383.17	10	-329.75	5	-265.80	5	-180.44	5
A5	303.52	1	277.54	1	248.87	1	216.44	1	178.19	1
A6	-322.13	6	-381.26	9	-432.38	10	-478.06	11	-519.74	11
A7	-307.90	5	-373.87	7	-429.83	9	-479.31	12	-524.13	12

A8	-366.85	8	-375.07	8	-383.12	7	-391.00	7	-398.72	8
A9	187.19	2	168.01	2	146.35	2	120.86	2	88.31	3
A10	-717.03	13	-638.37	13	-548.54	13	-440.77	9	-296.07	7
A11	-374.25	10	-445.39	12	-506.64	12	-561.24	13	-610.98	13
A12	-369.30	9	-404.88	11	-437.59	11	-468.02	10	-496.58	10
A13	40.95	4	68.67	4	88.06	4	103.90	3	117.62	2
	φ=3									
	α = 0.1		α = 0.3		α = 0.5		α = 0.7		α = 0.9	
	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank	Ω_i	Rank
A1	-397.88	11	-375.25	5	-349.49	5	-319.26	6	-281.85	6
A2	-337.56	7	-380.87	7	-416.08	8	-446.17	8	-472.66	9
A3	151.59	3	139.66	3	125.26	3	106.46	4	76.50	4
A4	-436.30	12	-401.96	10	-360.47	6	-306.28	5	-219.84	5
A5	306.15	1	285.03	1	260.20	1	229.43	1	186.97	1
A6	-333.83	6	-399.59	9	-448.82	10	-489.11	10	-523.68	11
A7	-323.02	5	-396.26	8	-449.36	11	-492.21	11	-528.68	12
A8	-367.06	8	-375.53	6	-383.64	7	-391.41	7	-398.89	8
A9	189.58	2	175.05	2	157.60	2	135.09	2	100.53	3
A10	-727.70	13	-670.27	13	-600.84	13	-510.05	12	-364.62	7
A11	-388.80	10	-467.92	12	-526.71	12	-574.69	13	-615.76	13
A12	-373.06	9	-411.95	11	-444.62	9	-473.08	9	-498.48	10
A13	57.33	4	82.88	4	98.313	4	110.00	3	119.63	2

This research undertakes comparative analyses to contrast the outcomes of the proposed approach with other PF-based approaches documented in the existing literature. The final rank of the risks based on the PF-ARTASI method has been compared with the PF-MOORA method to substantiate the validity of the derived outputs as well as the capability and efficacy of the proposed approach. As shown in Table 14, the PF-MOORA method, A5, A3, and A9 occupy the first, second, and third priority positions, respectively. Ultimately, the concluding ranking of cybersecurity risks associated with IoT applications within the retail sector, as determined by both methods, reveals a consistent set of critical risks that necessitate strategic planning for the implementation of corrective and preventive measures. Conversely, certain discrepancies exist in some prioritizations; for instance, based on the outcomes of the PF-ARTASI method, A4 is designated as the fifth priority, whereas in the PF-MOORA method and Figure 2, A10 holds the fifth priority position. Critical risks necessitate strategic planning for implementing corrective and preventive measures. The correlation coefficient for the proposed approach and PF-SWARA-MOORA is 0.758. These results confirm the validity of the proposed method, as the findings align with those of the PF-MOORA approach, which is recognized as a reliable method in the literature (Ghiaci & Ghoushchi, 2023). Consequently, it can be asserted that the proposed approach of this study is practical and represents a novel application within the domain of FMEA.

Table 14. Comparing the results of the PF-ARTASI approach with the PF-MOORA method

	PF-ARTASI		PF-MOORA	
	Ω_i	Rank	Score	Rank
A1	-333.50	6	-0.03	6
A2	-397.92	8	-0.32	10
A3	98.89	3	0.20	2
A4	-283.93	5	-0.05	7
A5	235.64	1	0.22	1
A6	-413.71	10	-0.46	12
A7	-407.04	9	-0.65	13
A8	-382.60	7	-0.18	8
A9	131.18	2	0.14	3
A10	-469.31	12	0.02	5
A11	-483.71	13	-0.43	11
A12	-430.21	11	-0.26	9
A13	55.68	4	0.13	4

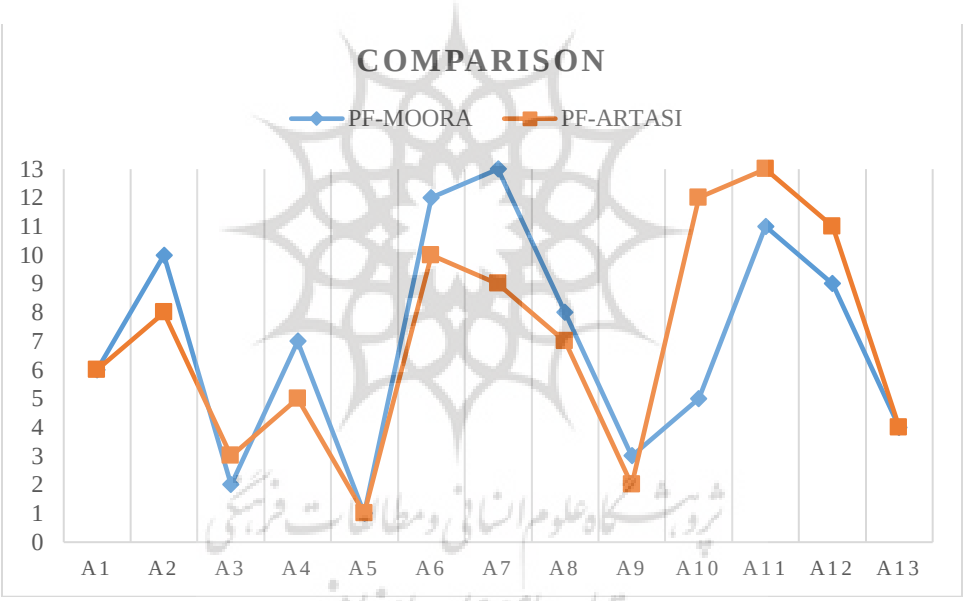

Figure 2. Comparison of the preference order of cybersecurity risks to IoT applications in the retail sector with various approaches

Conclusion

The IoT has introduced transformative opportunities for improving efficiency, innovation, and responsiveness in modern retail environments. However, the rapid expansion of interconnected devices has simultaneously intensified cybersecurity concerns related to data protection, system integrity, and user privacy, particularly in developing markets such as Iran, where retail infrastructures are undergoing fast digitalization but often lack unified security standards. To address these challenges, this study proposes a novel and fully integrated framework for identifying and prioritizing IoT-related cybersecurity risks in the retail sector. The framework combines PF-

SWARA and PF-ARTASI within the traditional FMEA structure, utilizing Pythagorean fuzzy sets to effectively capture uncertainty in expert judgments. By identifying failure scenarios through FMEA, deriving criteria weights via PF-SWARA, and ranking risks using PF-ARTASI, this research fills an important gap in the literature by presenting the first application of a PF-SWARA–ARTASI enhanced FMEA model tailored explicitly for cybersecurity assessment in IoT-enabled retail systems.

The PF-SWARA method was applied to determine the relative weights of the three FMEA criteria: Severity, Occurrence, and Detection. The results indicate that Severity has the most decisive influence on cybersecurity risk assessment in retail contexts, as security breaches can lead to substantial financial losses, operational disruptions, and reputational damage. Detection and Occurrence follow in importance, reflecting their essential yet comparatively lower roles. These findings are consistent with prior studies, including Alvand et al. (2023), Ghiaci and Ghoushchi (2023), and Maghami et al. (2024), all of which identify Severity as the dominant factor in risk evaluation. The use of Pythagorean fuzzy sets further enhances the reliability of expert judgments by reducing ambiguity and producing more stable weight estimates. This provides a solid and precise foundation for subsequent risk ranking and mitigation planning.

The PF-ARTASI method was then utilized to prioritize the identified cybersecurity risks. Through its adaptive two-level standardization and simultaneous comparison with ideal and anti-ideal solutions, PF-ARTASI enabled a clear and robust ranking of threats. The results showed that Insecure Firmware/Software and Lack of patch management represent the most critical risk factor, mainly due to the rapid upgrade cycles of IoT devices, which often leave systems outdated and susceptible to attacks (Aslan et al., 2023). Unpatched vulnerabilities may allow adversaries to impersonate devices, bypass surveillance, or compromise system integrity (Tariq et al., 2023). Even legitimate updates may introduce new weaknesses, underscoring the need for secure and well-governed patch management across all firmware and software layers (Hassija et al., 2019; Dejon et al., 2019).

The second most significant risk, Lack of Standardization and Interoperability Issues, stems from the fragmented nature of IoT ecosystems and inconsistent communication protocols (Roe et al., 2022; Ahmetoglu et al., 2022). Limited interoperability complicates device integration, increases operational workload, and restricts the implementation of consistent security controls. This fragmentation also weakens monitoring and incident response capabilities, intensifying legal and financial risks, particularly in areas such as data protection and transactional security (Brous et al., 2020; Verma et al., 2022).

Physical Security Threats were ranked third, emphasizing that the physical accessibility of IoT devices exposes them to direct manipulation. Threat actors can tamper with devices by cutting power, removing components, or attaching malicious hardware, thereby compromising system availability and integrity (Schiller et al., 2022; Tariq et al., 2023; Sadhu et al., 2022). Unauthorized physical access may also enable changes to firmware or configurations that circumvent digital safeguards. These findings underscore the importance of cybersecurity strategies that integrate digital protections with robust physical security controls.

The sensitivity analysis demonstrated that variations in the parameters φ and α did not result in significant deviations from the results. The relative ranking of risks remained largely stable across most scenarios, highlighting the robustness and reliability of the proposed PF-SWARA–PF-ARTASI model. Notably, Insecure Firmware/Software and Lack of Patch Management consistently ranked as the highest-priority risk in all scenarios, reaffirming the critical importance of secure software updates and systematic patch management in retail IoT systems.

In the comparative analysis, the PF-ARTASI results were contrasted with those obtained using the established PF-MOORA method. The findings revealed a strong alignment between the two approaches, with both consistently identifying Insecure Firmware/software, lack of Patch Management, Physical Security Threats, and Lack of Standardization and Interoperability Issues as the most critical risks. The calculated correlation coefficient of 0.758 further confirms a high level of consistency between the proposed approach and an established method in the literature. Minor discrepancies, such as ranking differences between Unauthorized Access to the IoT Network and Regulatory Compliance Challenges, indicate that PF-ARTASI offers greater sensitivity to variations in utility values. This enhanced sensitivity enables more precise differentiation of priorities among risks. Consequently, IT managers and policymakers can rely on this approach to allocate resources effectively, implement targeted mitigation strategies, and strengthen cybersecurity resilience in IoT-enabled retail environments.

In the existing body of research on IoT-related cybersecurity risks in retail, the importance of Insecure Firmware/Software and Lack of Patch Management has been widely acknowledged. Several studies, including those by Roe et al. (2022), Feng et al. (2022), Dejon et al. (2019), and Ozkan-Okay et al. (2024), highlight that inadequate patching, outdated firmware, and unaddressed software vulnerabilities substantially increase exposure to cyberattacks in interconnected retail and service infrastructures. Likewise, the critical role of Physical Security Threats has been repeatedly emphasized in prior work, such as Schiller et al. (2022), Aslan et al. (2023), Alsheikh et al. (2021), Rizvi et al. (2020), and Sadhu et al. (2022), which demonstrate how device tampering, hardware manipulation, or unauthorized physical access can compromise the integrity of the entire IoT ecosystem. Additionally, the challenges of Standardization and interoperability issues have been

clearly recognized in studies such as Gamil et al. (2020), Roe et al. (2022), and Birkel and Hartmann (2019), particularly in relation to fragmented architectures, heterogeneous communication protocols, and vendor-dependent compatibility gaps. However, while these studies primarily identify and qualitatively discuss such risks, the present research advances the field by providing a systematic and quantitative ranking of these threats within a unified decision-making framework. By integrating FMEA with PF-SWARA and PF-ARTASI under a Pythagorean fuzzy environment, this study offers a more discriminative and uncertainty-aware prioritization of IoT cybersecurity risks in retail settings than existing approaches based on conventional FMEA or single-stage fuzzy MCDM techniques.

A key methodological contribution of this study is the first-ever development and implementation of the ARTASI technique within a Pythagorean fuzzy environment, an innovative extension not previously reported in the literature. Building on this advancement, the study integrates PF-SWARA to derive fuzzy weights for the FMEA criteria. It employs the newly developed PF-ARTASI to rank the identified risks, thereby enabling the simultaneous use of Pythagorean fuzzy sets in both the criteria weighting and risk ranking stages. This novel three-layered configuration forms a highly robust decision-making structure that captures uncertainty more effectively and provides finer discrimination among risk levels. By jointly addressing expert judgment uncertainty, multi-criteria interactions, and subtle variations in utility values, the proposed framework fills a significant methodological gap in the literature. Consequently, it delivers substantially improved accuracy, stability, and discriminatory power compared with classical FMEA and existing hybrid models, offering practitioners, IT managers, and policymakers a more comprehensive and sensitive decision-support tool for enhancing cybersecurity resilience in IoT-driven retail environments.

The findings of this research provide actionable insights for retail managers, IT administrators, and cybersecurity planners. By identifying Insecure Firmware/Software and Lack of Patch Management as the most critical threats, the proposed model highlights the urgent need for structured update policies, automated patch deployment mechanisms, and continuous vulnerability monitoring in IoT-driven retail systems. Moreover, the high ranking of Lack of Standardization and Interoperability Issues indicates that retailers should prioritize adopting unified standards, vendor-agnostic architectures, and compliance frameworks to reduce integration failures. The identification of Physical Security Threats as a top-tier risk emphasizes that cybersecurity strategies must incorporate device-level safeguards, secure hardware design, controlled physical access, and real-time tamper detection. The proposed framework thus equips decision-makers with a systematic tool to allocate resources efficiently, prioritize investments, and design multilayered defense strategies in complex retail environments.

Despite its contributions, this study is subject to several limitations that open avenues for future research. First, expert evaluations were collected exclusively from the Iranian retail sector, which may limit the generalizability of the results to other geographical or industrial contexts. Expanding the expert pool to include international perspectives could provide more diverse insights. Second, the analysis focused on a predefined set of cybersecurity risks and FMEA criteria; future studies may incorporate additional technical, organizational, or behavioral factors. Third, while PF-SWARA and PF-ARTASI proved effective for weighting and ranking, integrating alternative hybrid MCDM techniques such as PF-BWM, PF-MARCOS, or CRITIC-combined approaches may offer complementary benefits. Ultimately, future research may extend the model to real-time IoT threat monitoring, predictive risk analytics, or digital-twin-based cybersecurity assessments, thereby enhancing dynamic decision-making capabilities

Data Availability Statement

Data available on request from the authors.

Acknowledgements

The authors would like to thank all the participants in the present study.

Ethical considerations

The authors have witnessed various ethical issues, including plagiarism, failure to obtain informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancy.

Funding

The authors received no financial support for this article's research, authorship, and/or publication.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work.

References

Abdullah Sani, H. A., & Jaafar, N. I. (2025). Exploring the impact of IoT on governance and public service transformation: evidence from Malaysia's public sector. *Smart and Sustainable Built Environment*. https://doi.org/10.1108/SASBE-10-2024-0453

Abu Al-Haija, Q., & Al-Dala'ien, M. A. (2022). ELBA-IoT: An ensemble learning model for botnet attack detection in IoT networks. Journal of Sensor and Actuator *Networks*, *11*(1), 18. https://doi.org/10.3390/jsan11010018

Adapa, S., Fazal-e-Hasan, S. M., Makam, S. B., Azeem, M. M., & Mortimer, G. (2020). Examining the antecedents and consequences of perceived shopping value through smart retail technology. *Journal of Retailing and Consumer Services*, *52*, 101901. https://doi.org/10.1016/j.jretconser.2019.101901

Aghazadeh, H., Mohammadi, M., Zadbar, H. (2018). Identifying and Comparing the Priority of Commercialization Services Required for Growing and Developing Companies Based in Tehran University Science and Technology Park. *Industrial Management Journal*, *10*(4), 525–550. https://doi.org/10.22059/imj.2019.264596.1007480

Ahmetoglu, S., Che Cob, Z., & Ali, N. A. (2022). A systematic review of Internet of Things adoption in organizations: Taxonomy, benefits, challenges and critical factors. *applied sciences*, *12*(9), 4117. https://doi.org/10.3390/app12094117

Akhilesh, K. B. (2019). Smart technologies—Scope and applications. In Smart Technologies: Scope and Applications (pp. 1–16). Singapore: Springer Singapore.https://doi.org/10.1007/978-981-13-7139-4_1

Akram, M., Ilyas, F., & Deveci, M. (2024). Interval rough integrated SWARA-ELECTRE model: An application to machine tool remanufacturing. *Expert Systems with Applications*, *238*, 122067. https://doi.org/10.1016/j.eswa.2023.122067

Alkan, N. (2024). Evaluation of sustainable development and utilization-oriented renewable energy systems based on CRITIC-SWARA-CODAS method using interval valued picture fuzzy sets. *Sustainable Energy, Grids and Networks*, *38*, 101263. https://doi.org/10.1016/j.segan.2023.101263

Alsheikh, M., Konieczny, L., Prater, M., Smith, G., & Uludag, S. (2021). The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. *IEEE Consumer Electronics Magazine*, *11*(3), 59–68. 10.1109/MCE.2021.3079635

Altubaishe, B., & Desai, S. (2023). Multi-criteria decision making in supply chain management using FMEA and hybrid AHP-PROMETHEE algorithms. *Sensors*, *23*(8), 4041. https://doi.org/10.3390/s23084041

Alvand, A., Mirhosseini, S. M., Ehsanifar, M., Zeighami, E., & Mohammadi, A. (2023). Identification and assessment of risk in construction projects using the integrated FMEA-SWARA-WASPAS model under fuzzy environment: a case study of a construction project in Iran. *International journal of construction management*, *23*(3), 392–404. https://doi.org/10.1080/15623599.2021.1877875

Amiri, M., Hosseini Dehshiri, S.J., Yousefi Hanoomandar, A. (2018). Determining the Optimal Combination of Larg Supply Chain Strategies Using SWOT Analysis, Multi-criteria Decision-making Techniques and Game Theory. *Industrial Management Journal*, *10*(2), 221–246. https://doi.org/10.22059/imj.2018.257030.1007420

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Argyropoulou, M., Garcia, E., Nemati, S., & Spanaki, K. (2024). The effect of IoT capability on supply chain integration and firm performance: an empirical study in the UK retail industry. *Journal of Enterprise Information Management*, *37*(3), 875–902. https://doi.org/10.1108/JEIM-06-2022-0219. https://doi.org/10.1108/JEIM-06-2022-0219

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Ayyildiz, E. (2022). A novel pythagorean fuzzy multi-criteria decision-making methodology for e-scooter charging station location-selection. *Transportation Research Part D: Transport and Environment*, *111*, 103459. https://doi.org/10.1016/j.trd.2022.103459

Balali, A., Moehler, R. C., & Valipour, A. (2022). Ranking cost overrun factors in the mega hospital construction projects using Delphi-SWARA method: An Iranian case study. *International Journal of Construction Management*, *22*(13), 2577–2585. https://doi.org/10.1080/15623599.2020.1811465

Behnia, F., Ahmadabadi, H. Z., Schuelke-Leech, B. A., & Mirhassani, M. (2023). Developing a fuzzy optimized model for selecting a maintenance strategy in the paper industry: An integrated FGP-ANP-FMEA approach. *Expert Systems with Applications*, *232*, 120899. https://doi.org/10.1016/j.eswa.2023.120899

Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management: An International Journal*, *24*(1), 39–61. https://doi.org/10.1108/SCM-03-2018-0142

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, *51*, 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Caro, F., & Sadr, R. (2019). The Internet of Things (IoT) in retail: Bridging supply and demand. *Business Horizons*, *62*(1), 47–54. https://doi.org/10.1016/j.bushor.2018.08.002

Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: a survey. *Wireless Personal Communications*, *115*(2), 1667–1693. https://doi.org/10.1007/s11277-020-07649-9

Chnina, K., & Daneshvar, S. (2024). Aggregation of Risk Management and Non-Parametric Models to Rank Failure Modes of Radio Frequency Identification Systems. *Applied Sciences*, *14*(2), 584. https://doi.org/10.3390/app14020584

Dejon, N., Caputo, D., Verderame, L., Armando, A., & Merlo, A. (2019). Automated security analysis of IoT software updates. In IFIP International Conference on Information Security Theory and Practice (pp. 223–239). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-41702-4_14

De Vass, T., Shee, H., & Miah, S. J. (2018). The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective. *Australasian Journal of Information Systems*, *22*. https://doi.org/10.3127/ajis.v22i0.1734

De Vass, T., Shee, H., & Miah, S. J. (2021). Iot in supply chain management: a narrative on retail sector sustainability. *International Journal of Logistics Research and Applications*, *24*(6), 605–624. https://doi.org/10.1080/13675567.2020.1787970

Đurđević, N., Labus, A., Barać, D., Radenković, M., & Despotović-Zrakić, M. (2022). An approach to assessing shopper acceptance of beacon triggered promotions in smart retail. *Sustainability*, *14*(6), 3256. https://doi.org/10.3390/su14063256

Feng, X., Zhu, X., Han, Q. L., Zhou, W., Wen, S., & Xiang, Y. (2022). Detecting vulnerability on IoT device firmware: A survey. *IEEE/CAA Journal of Automatica Sinica*, *10*(1), 25–41. https://doi.org/10.1109/JAS.2022.105860

Gamil, Y., A. Abdullah, M., Abd Rahman, I., & Asad, M. M. (2020). Internet of things in construction industry revolution 4.0: Recent trends and challenges in the Malaysian context. *Journal of Engineering, Design and Technology, 18*(5), 1091–1102. https://doi.org/10.1108/JEDT-06-2019-0164

Ghadimi, P., Donnelly, O., Sar, K., Wang, C., & Azadnia, A. H. (2022). The successful implementation of Industry 4.0 in manufacturing: An analysis and prioritization of risks in Irish industry. *Technological Forecasting and Social Change*, *175*, 121394. https://doi.org/10.1016/j.techfore.2021.121394

Ghasemi, M., Saadaat, M., & Ghollasi, O. (2019). Threats of social engineering attacks against security of Internet of Things (IoT). In Fundamental Research in Electrical Engineering: The Selected Papers of The First International Conference on Fundamental Research in Electrical Engineering (pp. 957-968). Springer Singapore. https://doi.org/10.1007/978-981-10-8672-4_73

Gheidar-Kheljani, J. & Roshandel, S. (2021). Risk Assessment Based on Total Efficient Risk Priority Number Using Data Envelopment Analysis. *Industrial Management Journal*, *13*(1), 131–154. https://doi.org/10.22059/imj.2021.310813.1007783

Ghiaci, A. M., & Ghoushchi, S. J. (2023). Assessment of barriers to IoT-enabled circular economy using an extended decision-making-based FMEA model under uncertain environment. *Internet of Things*, *22*, 100719. https://doi.org/10.1016/j.iot.2023.100719

Ghoushchi, S. J., Garg, H., Bonab, S. R., & Rahimi, A. (2023). An integrated SWARA-CODAS decision-making algorithm with spherical fuzzy information for clean energy barriers evaluation. *Expert Systems with Applications*, *223*, 119884. https://doi.org/10.1016/j.eswa.2023.119884

Görçün, Ö. F., Zolfani, S. H., & Çanakçıoğlu, M. (2022). Analysis of efficiency and performance of global retail supply chains using integrated fuzzy SWARA and fuzzy EATWOS methods. *Operations Management Research*, *15*(3), 1445–1469. https://doi.org/10.1007/s12063-022-00261-z

Haseeb, J., Mansoori, M., & Welch, I. (2021). Failure modes and effects analysis (FMEA) of honeypot-based cybersecurity experiment for IoT. In 2021 IEEE 46th Conference on Local Computer Networks (LCN) (pp. 645-648). IEEE. https://doi.org/10.1109/LCN52139.2021.9525010

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEE Access*, *7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

Ho, T., Nguyen, H., Dinh, H., Pham, H., Pham, P., & Tham, U. (2025). Understanding customer opinions on IoT applications implemented in the retail industry worldwide and its implications for businesses

in Vietnam. *Journal of Systems and Information Technology*, *27*(1), 146–172. https://doi.org/10.1108/JSIT-02-2024-0035

Jafarzadeh Ghoushchi, S., Shaffiee Haghshenas, S., Memarpour Ghiaci, A., Guido, G., & Vitale, A. (2023). Road safety assessment and risks prioritization using an integrated SWARA and MARCOS approach under spherical fuzzy environment. *Neural computing and applications*, *35*(6), 4549-4567 https://doi.org/10.1007/s00521-022-07929-4

Jamme, H. T., & Connor, D. S. (2023). Diffusion of the Internet-of-Things (IoT): A framework based on smart retail technology. *Applied Geography*, *161*, 103122. https://doi.org/10.1016/j.apgeog.2023.103122

Janatyan, N., Alavi, S., & Parvinian, M. (2025). A risk and reliability-based scheduling method for troubleshooting regulators in Gas pressure stations: A case study of Isfahan Gas company. *Industrial Management Journal*, *17*(4), 56–75. https://doi.org/ 10.22059/imj.2025.387414.1008211

Kamble, S. S., Gunasekaran, A., Parekh, H., & Joshi, S. (2019). Modeling the internet of things adoption barriers in food retail supply chains. *Journal of Retailing and Consumer Services*, *48*, 154–168. https://doi.org/10.1016/j.jretconser.2019.02.020

Kara, K., Yalçın, G. C., Kaygısız, E. G., Simic, V., Örnek, A. Ş., & Pamucar, D. (2024). A Picture Fuzzy CIMAS-ARTASI Model for Website Performance Analysis in Human Resource Management. *Applied Soft Computing*, *111826*. https://doi.org/10.1016/j.asoc.2024.111826

Kardani Malekinezhad, M., Rahimnia, F., Eslami, G., & Farahi, M. M. (2025). Human resource analytics adoption: a framework-based analysis, fuzzy Delphi method and fuzzy SWARA. *Journal of Advances in Management Research*. https://doi.org/10.1108/JAMR-05-2024-0181

Kaur, M., Alzubi, A. A., Walia, T. S., Yadav, V., Kumar, N., Singh, D., & Lee, H. N. (2023). EGCrypto: a low-complexity elliptic galois cryptography model for secure data transmission in IoT. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3305271

Kaushik, K., & Dahiya, S. (2018). Security and privacy in IoT based e-business and retail. In 2018 International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 78–81). *IEEE*. https://doi.org/10.1109/SYSMART.2018.8746961

Khalil, G., Doss, R., & Chowdhury, M. (2020). A novel RFID-based anti-counterfeiting scheme for retail environments. *IEEE Access*, *8*, 47952–47962. https://doi.org/10.1109/ACCESS.2020.2979264

Li, X., Li, H., Sun, B., & Wang, F. (2018). Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA. *Journal of Intelligent & Fuzzy Systems*, *34*(4), 2491-2501. https://doi.org/10.3233/JIFS-172097

Lorente-Martínez, J., Navío-Marco, J., & Rodrigo-Moya, B. (2020). Analysis of the adoption of customer facing InStore technologies in retail SMEs. *Journal of Retailing and Consumer Services*, *57*, 102225. https://doi.org/10.1016/j.jretconser.2020.102225

Ma, B. J., Zhang, Y., Liu, S., Jiang, Y., He, Y., & Yan, K. (2022). Operational strategies for IoT-enabled Brick-and-Mortar retailers in a competitive market. *Computers & Industrial Engineering*, *173*, 108665. https://doi.org/10.1016/j.cie.2022.108665

Maghami, M. R., Vahabzadeh, S., Mutambara, A. G. O., Ghoushchi, S. J., & Gomes, C. (2024). Failure analysis in smart grid solar integration using an extended decision-making-based FMEA model under uncertain environment. *Stochastic Environmental Research and Risk Assessment*, *38*(9), 3543–3563. https://doi.org/10.1007/s00477-024-02764-6

Mock, R. G., López de Obeso, L., Zipper, C., & Schönenberger, M. (2016). Resilience assessment of internet of things: A case study on smart buildings. In Proceedings of the 26th European Safety and Reliability Conference (ESREL 2016) (pp. 2260–2267).

Mohammadzadeh, A. K., Ghafoori, S., Mohammadian, A., Mohammadkazemi, R., Mahbanooei, B., & Ghasemi, R. (2018). A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran. *Technology in Society*, *53*, 124–134. https://doi.org/10.1016/j.techsoc.2018.01.007

Nazari-Shirkouhi, S., & Zarei Babaarabi, R. (2025). Enhancing decision-making in healthcare systems: lean, agile, resilient, green, and sustainable (LARGS) paradigm for performance evaluation of hospital departments under uncertainty. *Industrial Management Journal*, *17*(2), 85–116. https://doi.org/10.22059/imj.2025.386420.1008208

Nayak, P., & Swapna, G. (2023). Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview. *Internet of Things*, *21*, 100641. https://doi.org/10.1016/j.iot.2022.100641

Okeke, R. I., & Eiza, M. H. (2023). The Application of role-based framework in preventing internal identity theft related crimes: A qualitative case study of UK retail companies. *Information Systems Frontiers*, *25*(2), 451–472. https://doi.org/10.1007/s10796-022-10326-w

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEE Access*, *12*, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547

Pamucar, D., Simic, V., Görçün, Ö. F., & Küçükönder, H. (2024). Selection of the best Big Data platform using COBRAC-ARTASI methodology with adaptive standardized intervals. *Expert Systems with Applications*, *239*, 122312. https://doi.org/10.1016/j.eswa.2023.122312

Parra-Sánchez, D. T. (2025). Exploring the Internet of Things adoption in the Fourth Industrial Revolution: a comprehensive scientometric analysis. *Journal of Innovative Digital Transformation*, *2*(1), 1–18. https://doi.org/10.1108/JIDT-06-2024-0013

Park, J. S., Ha, S., & Jeong, S. W. (2021). Consumer acceptance of self-service technologies in fashion retail stores. *Journal of Fashion Marketing and Management: An International Journal*, *25*(2), 371–388. https://doi.org/10.1108/JFMM-09-2019-0221

Pino, A. F. S., Ruiz, P. H., Mon, A., & Collazos, C. A. (2024). Mechanisms for measuring technology maturity on the Internet of Things in enterprises: A systematic literature mapping. *Internet of Things, 101100*. https://doi.org/10.1016/j.iot.2024.101100

Rahnamay Bonab, S., & Osgooei, E. (2025). Environment risk assessment of wastewater treatment using FMEA method based on Pythagorean fuzzy multiple-criteria decision-making. *Environment, Development and Sustainability*, *27*(9), 22185–22215. https://doi.org/10.1007/s10668-022-02555-5

Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, *11*, 100240. https://doi.org/10.1016/j.iot.2020.100240

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

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of things: Security and solutions survey. *Sensors*, *22*(19), 7433. https://doi.org/10.3390/s22197433

Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, *76*, 5320–5363. https://doi.org/10.1007/s11227-019-02945-z

Sarvari, H., Baghbaderani, A. B., Chan, D. W., & Beer, M. (2024). Determining the significant contributing factors to the occurrence of human errors in the urban construction projects: A Delphi-SWARA study approach. *Technological Forecasting and Social Change*, *205*, 123512. https://doi.org/10.1016/j.techfore.2024.123512

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467.

Serral, E., Vander Stede, C., & Hasić, F. (2020, June). Leveraging IoT in retail industry: a maturity model. In 2020 IEEE 22nd Conference on Business Informatics (CBI) (Vol. 1, pp. 114–123). IEEE. https://doi.org/10.1109/CBI49978.2020.00020

Sivaselvan, N., Bhat, K. V., Rajarajan, M., Das, A. K., & Rodrigues, J. J. (2023). SUACC-IoT: Secure unified authentication and access control system based on capability for IoT. *Cluster Computing*, *26*(4), 2409–2428. https://doi.org/10.1007/s10586-022-03733-w

Soltanali, H., & Ramezani, S. (2023). Smart failure mode and effects analysis (FMEA) for safety–Critical systems in the context of Industry 4.0. In Advances in Reliability, Failure and Risk Analysis (pp. 151–176). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-9909-3_7

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy, and efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, *19*, 174–184. https://doi.org/10.1016/j.suscom.2018.06.003

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

Tian, Y., Song, S., Zhou, D., Pang, S., & Wei, C. (2023). Canonical triangular interval type-2 fuzzy set linguistic distribution assessment TODIM approach: A case study of FMEA for electric vehicles DC charging piles. *Expert Systems with Applications*, *223*, 119826. https://doi.org/10.1016/j.eswa.2023.119826

Uddin, M. R., Akter, S., & Lee, W. J. T. (2024). Developing a data breach protection capability framework in retailing. *International Journal of Production Economics*, *271*, 109202. https://doi.org/10.1016/j.ijpe.2024.109202

Verma, A., Verma, P., Farhaoui, Y., & Lv, Z. (Eds.). (2022). Emerging real-world applications of internet of things. CRC Press. DOI: 10.1201/9781003304203

Waqas, M., Kumar, K., Laghari, A. A., Saeed, U., Rind, M. M., Shaikh, A. A., ... & Qazi, A. Q. (2022). Botnet attack detection in Internet of Things devices over cloud environment via machine learning. *Concurrency and Computation: Practice and Experience*, *34*(4), e6662. https://doi.org/10.1002/cpe.6662

Wazid, M., Das, A. K., Hussain, R., Succi, G., & Rodrigues, J. J. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. *Journal of Systems Architecture*, *97*, 185–196. https://doi.org/10.1016/j.sysarc.2018.12.005

Yaftiyan, F., Saghafi, F., & Hosseinzadeh, M. (2025). Analyzing key variables in recurrent carbon reduction policies using a hybrid approach: A focus on pharmaceutical distributors in Iran. *Industrial Management Journal*, *17*(2), 1–26. https://doi.org/10.22059/imj.2025.392285.1008233

Yager, R. R. (2013). Pythagorean fuzzy subsets. In 2013 joint IFSA world congress and NAFIPS annual meeting (IFSA/NAFIPS) (pp. 57–61). *IEEE*. https://doi.org/10.1109/IFSA-NAFIPS.2013.6608375

Yalçın, G. C., Kara, K., & Senapati, T. (2024). A hybrid spherical fuzzy logarithmic decomposition of criteria importance and alternative ranking technique based on Adaptive Standardized Intervals model with application. *Decision Analytics Journal*, *11*, 100441. https://doi.org/10.1016/j.dajour.2024.100441

Younis, H., Shbikat, N., Bwaliez, O. M., Hazaimeh, I., & Sundarakani, B. (2025). An overarching framework for the successful adoption of IoT in supply chains. Benchmarking: An International Journal.De Andrade, P. R., Patuzzo, G. V., & Cardoso, F. A. R. (2025). Industrial management: implementation of the TPM tool in a coffee industry. *Brazilian Journal of Production Engineering*, *11*(1), 166–191. https://dx.doi.org/10.47456/bjpe.v11i1.46368

پرتال جامع علوم انسانی