Vol 17, Fall and Winter 1403

Information Technology in Engineering Design

https://sanad.iau.ir/journal/ited

Exploring the Key Factors Impacting Dependability Evaluation Parameters in IoT Systems for Healthcare Domain

Ali Kosari[(1)] Esmaeil Kheirkhah[(2)*] Seyyed Reza Kamel Tabbakh Farizani[(3)]

(1) Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran
(2) Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran*
(3) Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran

(Date received: 1402/11/09 Date accepted: 1403/05/01)

Abstract

In the healthcare domain, advancements in technology and medical research have propelled significant progress, leveraging the capabilities of the Internet of Things (IoT) for diagnosing, treating, and monitoring human diseases. From cutting-edge imaging scanners to intelligent surgical robots, IoT systems in healthcare have elevated therapeutic precision and accuracy through the integration of advanced technology and scientific innovations. However, ensuring the reliable and satisfactory performance of IoT systems in healthcare is paramount for gaining the trust of physicians, operators, and patients. Dependability has thus emerged as a pivotal factor in the design and development of IoT systems within the healthcare domain. Nevertheless, challenges related to dependability persist in healthcare IoT systems. This article employs the Delphi and Snowball Sampling methods to investigate the factors influencing dependability in IoT systems within the healthcare domain. By aggregating expert opinions and experiences, a conceptual method illustrating the factors impacting dependability in healthcare IoT systems has been formulated. The findings aim to contribute to enhancing device dependability during the design and development phases of healthcare IoT systems. The findings of this article indicate that the most influential factors affecting the assessment of the dependability of healthcare systems are reliability, safety, and confidentiality. The factors impacting each of these parameters have been identified. The significance of these findings lies in improving patient monitoring and supervision, enabling rapid disease diagnosis and prevention, advancing diagnostic and therapeutic capabilities, optimizing resource management in healthcare provisions, and preserving patients' privacy.

Keywords: Evaluation parameters, Dependability, Healthcare, Internet of Things (IoT), IoT systems.

Corresponding author:
*Esmaeil Kheirkhah

Address: Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran
Email: e.kheirkhah@gmail.com

1- Introduction

In the contemporary landscape of medical technology, the Internet of Things (IoT) has emerged as a pivotal innovation. IoT entails a network of sensor-embedded objects capable of perceiving environmental conditions and, in certain applications, monitoring the physiological states of patients. These systems predominantly rely on wireless communication for connectivity to broader networks, such as the Internet, and process data through dedicated servers. Ensuring the reliable performance of these devices is paramount to mitigating risks to human health and the environment. Any lapses or vulnerabilities in dependability can potentially expose patients, healthcare providers, and the surrounding environment to significant hazards.

The widespread adoption and diverse deployment of IoT devices in medical contexts, compounded by the absence of standardized protocols and frameworks, have introduced numerous challenges and vulnerabilities. Ensuring dependability thus represents a fundamental challenge within this domain, necessitating a thorough investigation into evaluation parameters and their influencing factors. This article endeavors to explore the influential factors affecting the assessment parameters of dependability in IoT systems within the healthcare sector.

By employing a hybrid methodology that integrates the Delphi technique with Snowball Sampling, this research aims to systematically gather and synthesize expert opinions on these influencing factors. The reliability and validity of this methodological approach will be rigorously assessed using established methodologies.

Structurally, this article is designed to comprehensively address the intricacies of ensuring dependability in IoT systems within healthcare settings. It commences with an extensive exploration of the research background and relevant literature, elucidating fundamental concepts and showcasing case studies that underscore critical evaluation parameters and influencing factors impacting reliability assessments. The proposed hybrid method combines the Delphi technique for expert consensus building with Snowball Sampling for comprehensive data collection, thereby offering a robust framework to identify and evaluate factors specific to enhancing IoT dependability in healthcare contexts. The subsequent results and discussion section will synthesize findings derived from this study, analyzing identified factors and their implications for augmenting the reliability of IoT systems in medical environments. Finally, the conclusion will consolidate key insights and contributions, emphasizing the significance

of these findings in guiding the design and development of more dependable healthcare technologies.

2- Research Background And Literature Review

The Internet of Things (IoT) has become a prominent focus in medical technology, comprising a network of sensor-equipped objects capable of environmental perception and, in some cases, monitoring a patient's internal conditions. These systems utilize wireless communication to connect to extensive networks such as the Internet and process information through servers. The diversity and widespread adoption of these devices in medicine, alongside the absence of standardized protocols, frameworks, and common standards, have introduced significant challenges and errors. Dependability emerges as a critical challenge in this domain. Addressing it requires identifying evaluation parameters and comprehending the influencing factors. This article explores influential factors affecting dependability evaluation parameters and proposes a hybrid method using Snowball Sampling and Delphi techniques to systematically collect and synthesize these factors. Finally, the method's reliability and validity are assessed using appropriate methodologies.

To establish a common understanding of dependability, definitions from relevant literature are provided. Knight [1], in 2012, defined dependability as "the capacity of a system to prevent service failures that occur more frequently and with greater severity than is deemed acceptable." According to Knight [1], the foundation for determining the dependability requirements of any system rests on a set of six attributes derived from a taxonomy (see Table 1).

This structured approach ensures a comprehensive examination of dependability in IoT systems within healthcare, enhancing our ability to mitigate risks and improve reliability in medical technology applications.

Table 1: Dependability Evaluation Parameters

Parameter	Description
Reliability	Continuity of correct service
Availability	Readiness for correct service
Safety	Absence of catastrophic consequences on the user(s)
Integrity	Absence of improper system alterations
Confidentiality	Absence of unauthorized disclosure of information
Maintainability	Ability to undergo modifications and repairs

In the healthcare sector, dependability, as defined by Whig et al. [2] in their recent article, encompasses the proficiency of medical systems and equipment to execute tasks related to patient diagnosis, treatment, or monitoring reliably and without errors. It ensures the consistent and stable performance of medical devices to deliver accurate and secure healthcare services. A dependable medical device operates continuously, providing reliable results and minimizing the risk of errors or failures that could impact patient care. The critical role of dependability in healthcare cannot be overstated, as it is integral to maintaining the integrity and effectiveness of medical procedures and interventions.

Reliability is defined as the probability of correct operation of a medical system or device in a specific environment until a designated time. This concept refers to the likelihood that a medical device or system will perform its tasks accurately and without errors related to diagnosis, treatment, or patient monitoring within a specified timeframe [3].

Safety in medical devices involves providing healthcare services without risks or harm to patients, healthcare professionals, and the surrounding environment, adhering to safety measures to prevent accidents or adverse events [4].

Confidentiality in medical devices safeguards patients' personal and sensitive information, ensuring privacy and access only to authorized individuals through technologies like encryption and security policies [5].

The primary goal of this study is to enhance service quality and improve the dependability of IoT systems in healthcare. Table 2 presents some of the most important dependability evaluation parameters, which can be effective in assessing the system's dependability.

Table 2: Dependability Evaluation Parameters used in this paper

Parameter	Description
Reliability	The probability of correct system operation in a specific environment until time t. [6,7]
Safety	The system should not pose a catastrophic risk to users or its surrounding environment. [7,8]
confidentiality	The system should not allow unauthorized intentional or unintentional changes. [9-11]

Creating a successful and reliable IoT system entails systematic planning to discern user needs and system objectives. This encompasses identifying the user demographics, specifying the requirements of patients or medical professionals, and elucidating their goals. Following the planning phase, hardware and software design involves the meticulous selection of critical components in hardware, such as sensors and

microcontrollers, and considerations in software, including programming languages and communication protocols. System improvement necessitates the simultaneous development and integration of both hardware and software components. The subsequent phase comprises comprehensive testing, including performance evaluation, data validation, communication, and security testing. After the initial cycle, the system is deployed, accompanied by support services like distribution, assistance, upgrades, and updates for both software and hardware. Proactive measures are taken to address any arising errors or issues. Designing and developing IoT systems demands collaboration among diverse teams, proficiency in various domains, and the judicious selection of evaluation parameters. Ensuring system dependability requires a methodical analysis of factors influencing these parameters [12]. The proposed method in this paper offers the advantage of identifying needs and objectives, designing appropriately, and selecting evaluation parameters. However, its disadvantages include time and cost implications, complexity in management, and a lack of accurate recognition of evaluation factors.

The convergence of IoT, cloud computing, and big data has led to substantial progress in the healthcare sector, notably in the evolution of smart healthcare and IoT systems. In IoT-based smart healthcare, patients can collect their vital signs using medical sensors attached to their bodies, facilitating disease detection and automatic preliminary diagnosis. However, the shared use of computational resources in the cloud platform by these medical devices may lead to competition and unintentional disruptions in service performance among patients. In their study, Zhang et al. [13] identified that addressing the challenges of isolating service provisioning among patients and ensuring Service Level Agreements (SLA) for both patients and cloud service providers is crucial and warrants careful attention and investigation. Improving service quality, increasing patient satisfaction, and reducing risk are among the advantages of their approach. One of its disadvantages includes the complexity of SLA regulations and the need to determine individual responsibilities.

In 2022, Wu et al. [14] conducted a study on upper limb prosthetics, revealing that existing prosthetics do not fully cater to users' needs. Challenges, such as insufficient training and incomplete communication channels between users, physicians, and prosthetic manufacturers, hinder the effective utilization of available quantitative and qualitative data for prosthetic improvements. The study employed IoT communications, remote data collection, real-time visualization, and cloud-based prosthetic reprogramming via Wi-Fi and a commercial cloud portal for user communication and training. Users can adjust device settings and provide additional background information through a dashboard. The authors' primary objective is to develop more suitable prosthetics by utilizing background data collection, internet-based system updates, and

enhanced training and communication with users. These advantages contribute to the refinement of prosthetic devices, facilitating remote monitoring, adjustments, and user education for an improved user experience and satisfaction. However, their approach encounters challenges related to communication complexity, network disruptions, and increased maintenance costs.

In healthcare applications, the evaluation of Quality of Service (QoS) plays a crucial role in processing medical records using intelligent measurement methods. Khan et al. [15] addressed this issue in their article titled "Smart Contracts and Metaheuristics for Secure Quality-of-Service and Cost-Efficient Scheduling of Medical-Data Processing" from three perspectives. Firstly, they proposed a metaheuristic approach for cost planning in healthcare programs, managed by an intelligent planner utilizing Fog Nodes. Secondly, they developed an algorithm for calculating QoS efficiency through Quality of Experience (QoE) analysis. Lastly, they introduced a QoS-ledger framework using blockchain-broadcast technology in public peer-to-peer (PTP) networks, ensuring secure storage of medical information. Simulation results indicated improvements in transmission capability, reduced jitter and latency, and increased transmission speed. The challenges of their approach can include process complexity, network deficiencies, and maintenance costs.

Transportation plays a vital role in people's daily lives and reflects societal development. However, recent years have seen an increase in risk factors such as drowsiness, lack of attention, unauthorized speeding, and reckless substance use, posing threats to the lives of both drivers and others. In a 2022 study, Uma et al. [16] utilized various sensors, including eye movement monitoring, detection of neck bending, and identification of false odors and toxic gases, to provide timely alerts to prevent hazardous incidents. The findings emphasize the crucial role of monitoring and regulating driver behavior in ensuring the safety of both the vehicle and its occupants.

Closely monitoring the inappropriate behavior of patients in their surroundings is paramount for reducing environmental and device-related risks. By observing and supervising patient behavior, potential hazards can be identified and addressed promptly. This monitoring is effective in preventing accidents, ensuring the safety of both patients and those nearby, and maintaining the proper functioning of surrounding devices. A study by Khan et al. [17] emphasized the significant role of such monitoring in preventing incidents, ensuring patient and bystander safety, and preserving the optimal performance of surrounding devices. Implementing robust monitoring systems and effective protocols in healthcare settings is crucial for maintaining a safe and secure environment for patients and healthcare providers.

Regulations and standards are pivotal for the widespread acceptance and adoption of

emerging technologies. Additive Manufacturing (AM), also known as 3D printing, is an innovative technology rapidly advancing and influencing various industries, particularly in healthcare and medicine. Given the sensitivity and complexity of this domain, specific regulations, standards, and protocols have been developed and implemented. In the article titled "Regulatory and Standards Development in Medical Additive Manufacturing," authored by Rafi et al. in 2022 [18], the authors thoroughly examine the standards and protocols within this field. Their conclusion emphasizes that the implementation of these standards and regulations in devices reduces the gap between devices and enhances their efficiency.

Healthcare IoT systems encompass a diverse range of products, including sensor-equipped gloves and digital dermatoscopes, and are now subject to a new legal framework in the European Union, effective from May 2021. The implementation of these regulations has a notable qualitative impact on healthcare IoT system providers, as well as dermatologists and physicians. The regulations entail the reclassification of software and applications utilized in healthcare IoT systems, coupled with more stringent requirements for related documentation. As highlighted by the authors of the article [19], these updates are anticipated to positively influence the quality and safety of patient care. However, it is important to acknowledge that they may also lead to increased prices.

The objective of Tuska and colleagues in their 2023 article [20] was to analyze the efforts of the Ministry of Health of Brazil in managing medical equipment, specifically focusing on lung ventilation devices in the context of the COVID-19 pandemic. The results of the article demonstrate that the Ministry of Health of Brazil plays a crucial role in ensuring healthcare systems, highlighting its prominent function as a national policy coordinator in health technology management. According to the mentioned national policy, the Ministry of Health is required to support health managers in the implementation, monitoring, and maintenance of healthcare technologies. Within less than a year, the Ministry of Health has procured a significant number of lung ventilation devices, amounting to 8.55 times the annual average of equipment acquired during the period from 2016 to 2019.

In 2023, Liu and colleagues [21] introduced a new scheme aimed at preserving privacy in the Industrial Internet of Things (IIoT) system. Their proposed method has demonstrated resilience against file injection attacks and has proven effective in withstanding such security threats. During search operations, users only receive a specific attribute value based on their access level, rather than the entire file. Their approach reduces communication costs and minimizes the disclosure of patients' privacy.

Table 3: Summary table of advantages and disadvantages of literature review

Category	Advantages	Disadvantages	References
Development of IoT Systems in Healthcare	Development and management of IoT systems in healthcare help in the continuous improvement of healthcare services. Using IoT prosthetics and sensors in medicine facilitates better patient monitoring and disease diagnosis. Implementation of new EU regulations on IoT systems in healthcare ensures improved data reliability and safety.	Complexity in management and high costs for developing and implementing IoT systems in medical environments. Need for precise standards and methods to address security and privacy challenges when using sensitive patient data.	[12-14,19]
Use of IoT Systems in Accidents and Hospitals	Use of sensors for patient monitoring and preventing accidents and incidents in hospitals. Plays a significant role in enhancing patient safety and improving healthcare services.	Complexity in implementing monitoring systems and the need for advanced infrastructure for communications and data transmission.	[16,17]
Use of IoT Systems in Health Technology Management and Pandemic Response	Development of standards and regulations in the production and use of medical technology during special conditions like the COVID-19 pandemic. Improvement in the quality of healthcare services and better management of medical technologies.	Complexity in implementing regulations and the need for resources to support and monitor the implementation of standards.	[18,20]
Privacy Preservation in Industrial IoT Systems	Preservation of privacy and security of sensitive data in industrial IoT systems, such as those used in critical sectors.	Complexity in implementing and managing data security and privacy in industrial environments.	[21]
Quality of Service Evaluation in Medical Data Processing	Use of smart contracts and blockchain technology to improve the quality of services in medical data processing.	Complexity in implementing smart contracts and the need for advanced infrastructure to utilize blockchain technology in medical environments.	[15]

In Table 3, the categorization and summary of the literature review are presented. As you can see, the advantages and disadvantages of the literature review are listed in this table.

This section primarily focuses on the challenges and advancements associated with IoT in the field of healthcare. Initially, fundamental concepts such as dependability, reliability, safety, and confidentiality in medical systems using IoT were thoroughly examined. Subsequently, multiple case studies were presented, each highlighting one or two reliability assessment parameters and the influencing factors on these parameters. It was emphasized that these factors can have significant impacts on safety, quality, and healthcare service costs. Consequently, there is a growing need to propose a method for ensuring the dependability of IoT systems to develop and implement resilient systems. Such a method aims to enhance healthcare services for both patients and healthcare professionals by addressing the identified challenges and leveraging the opportunities presented by IoT in the healthcare domain.

3- Proposed Method

By the preceding section, numerous endeavors have been dedicated to addressing the concept of dependability, each focusing on the examination of at most two parameters associated with dependability assessment or a limited set of influencing factors. While each approach has contributed to advancements in specific domains, none has proposed a comprehensive solution for ensuring the overall dependability of systems. The consideration of all assessment parameters, along with their associated factors, may introduce complexity and high costs in the context of IoT systems. Conversely, a reduction in the number of parameters could potentially lead to irreparable risks for the system. Hence, there exists a compelling need for the development of a comprehensive method that, based on expert opinions, formulates a holistic framework for the creation of dependable systems. Such a method aims to strike a balance between thorough evaluation and practical implementation, ensuring both reliability and feasibility.

This section delineates the methodology employed for the systematic collection, examination, and identification of all pertinent factors influencing dependability. Additionally, it aims to establish a clear relationship between each identified factor and the assessment parameters associated with dependability.

The proposed method's process is depicted in Fig. 1, integrating a hybrid approach of the Snowball Sampling method and the Delphi method. Firstly, the author assembles a preliminary list of key factors influencing IoT devices. Next, a specific group of experts is identified to generate an initial list of factors that impact the evaluation parameters of

IoT. The process then incorporates the Snowball Sampling method, a technique where additional factors are identified based on recommendations or inputs from the initial group of experts. This iterative process continues until a comprehensive set of factors is compiled, forming the basis for a thorough analysis of the influential elements on the evaluation parameters of IoT. This hybrid approach ensures that the method is both exhaustive and inclusive, capturing a wide range of expert insights and empirical data to inform the development of dependable IoT systems.

3-1- The Snowball Sampling Stage

Snowball sampling is a non-probability sampling technique that commences with the identification of an initial group of individuals. The sample is subsequently broadened by integrating more individuals through the social networks and personal connections of those already included in the sample. This method proves beneficial for incorporating individuals who could be difficult to reach directly, either because of restricted access to the community or the limited presence of individuals within the desired community [22-24].

In the snowball sampling method, experts are allowed to recommend additional experts or authorities, thereby improving the effectiveness of the expert panel. The incorporation of more experts expedites the identification of new data and factors for the system. In this study, experts were not only requested to furnish information on factors influencing the dependability evaluation parameters of IoT systems but were also motivated to introduce new experts to the system.

Researchers suggest a cohort of ten experts for the administration of questionnaires, especially when respondents are individuals with expertise, such as managers and professors, who possess knowledge and opinions in their respective fields. In situations where the number of available experts is below ten, the existing experts can be consulted to propose additional experienced individuals, thereby broadening the participant pool.

To discern the most impactful factors influencing evaluation parameters, expert opinions are sought. Experts are welcome to put forward new influential factors, and if they are cognizant of experienced individuals who can contribute to this identification process, they are urged to nominate them. This iterative process persists until no new influential factors or additional experienced experts are recognized.

Subsequently, in the section labeled "Monitoring Factors," a team of experts is entrusted with the responsibility of integrating, eliminating, or consolidating multiple influential factors as needed. Moreover, they are asked to furnish standardized definitions for each evaluation parameter. This ensures a comprehensive and precise understanding

of each factor's role and relevance in the dependability evaluation of IoT systems.

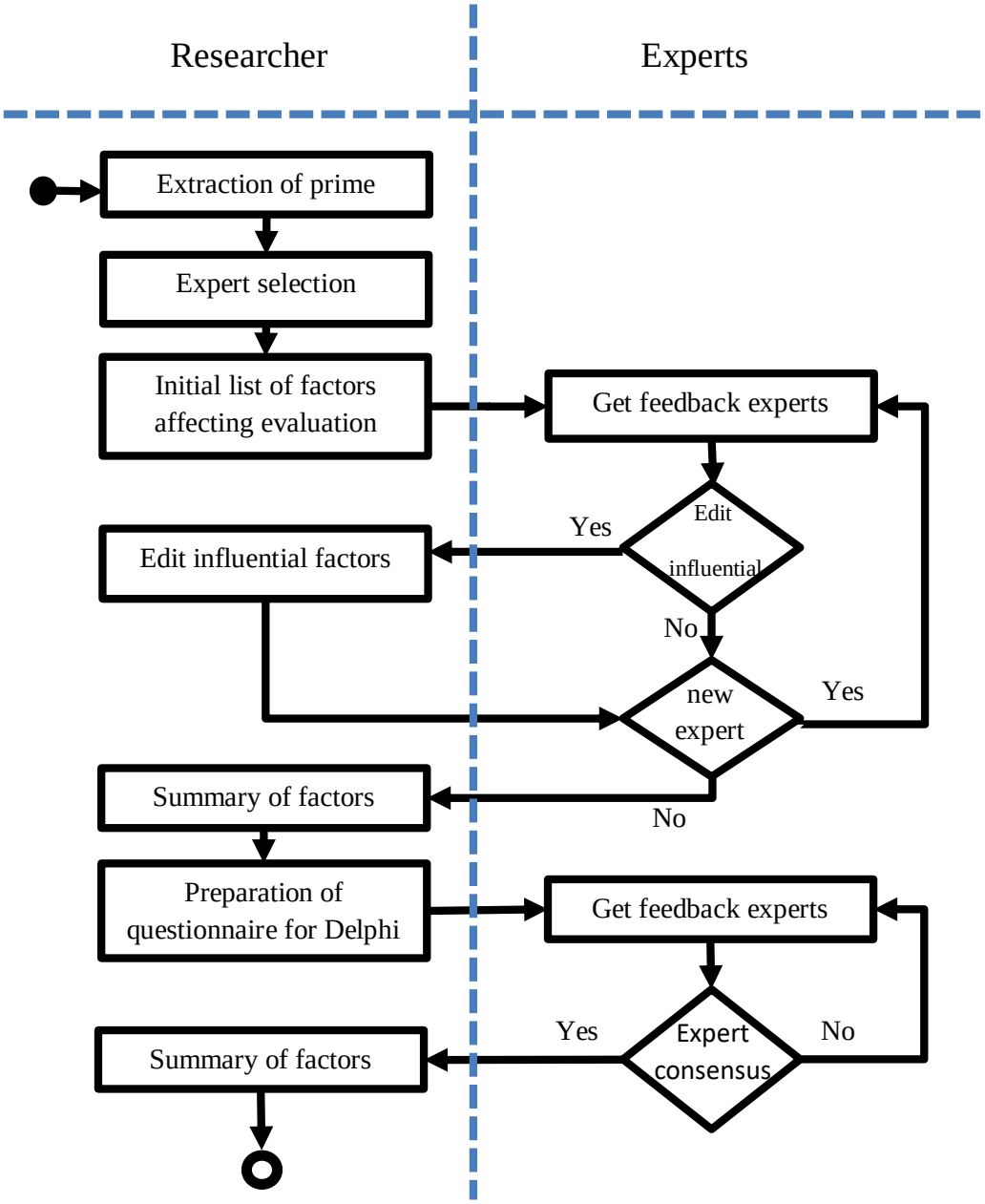

Figure 1: The process of extracting factors influencing the evaluation parameters of the IoTs in healthcare domain

3-2- Delphi Stage

The Delphi research method is a qualitative approach used to explore the opinions and perspectives of experts, specialists, or industry professionals. This method is applied in various research fields, including health, technology, management, economics, humanities, and more. It involves collecting participants' opinions through carefully designed questions that focus on specific topics under investigation. In the initial round, questions are posed to identify key points related to the subject. In subsequent rounds, participants receive feedback from the previous round, allowing them to review and make necessary adjustments to their opinions. The Delphi research method is particularly valuable in research that requires gathering expert opinions on a specific topic, and it proves highly effective in generating insightful insights [25-27].

Following the summarization of factors influencing IoT systems, electronic questionnaires were developed, consisting of three sections: 1) Reliability, 2) Safety, and 3) Confidentiality. Each section contained questions addressing the degree of correlation between these factors and the corresponding evaluation parameter. Experts were tasked with assessing the level of correlation for each factor with the reliability parameter, using response options ranging from No correlation to Very strong correlation, as detailed in Table 3. Additionally, a text box allowed experts to provide any necessary comments or essential points.

The questionnaires were distributed simultaneously among the experts, and upon receiving responses from all participants, the process advanced to the next phase. Subsequently, opinions and responses were anonymously shared with all participants. Following necessary revisions based on received feedback and obtaining responses from experts again, the questionnaire underwent further review.

Table 4: Responses for Each Factor in the Questionnaire

Value	Priority	Description
1	No correlation	The Priority does not correlate with the evaluation parameter.
2	Weak correlation	The Priority has a weak correlation with the evaluation parameter.
3	Moderate correlation	The Priority has a moderate correlation with the evaluation parameter.
4	Strong correlation	The Priority has a strong correlation with the evaluation parameter.
5	Very strong	correlation The Priority has a very strong correlation with the evaluation

In conclusion, upon achieving consensus among the experts, the Delphi method concludes its iterative process.

Throughout this study, a robust framework has been established by integrating the Snowball and Delphi methods. This framework facilitated the systematic collection and evaluation of influential factors affecting the dependability of IoT systems within the

healthcare domain. By leveraging the Snowball method initially to expand the list of factors and subsequently employing the Delphi method to refine and finalize these factors, the study ensured comprehensive coverage and expert validation. This integrated approach provided a unified method to explore the breadth and depth necessary for a thorough analysis of factors influencing IoT system dependability in healthcare. Ultimately, this method contributes to the development of sustainable IoT systems and the enhancement of healthcare services based on expert insights.

Dependability is crucial in medical systems, playing a pivotal role in ensuring device safety and effectiveness for patient health improvement. Addressing these factors is paramount when designing IoT systems in healthcare.

The next section will undertake a review and evaluation of the proposed method using Excel and SPSS software on Windows 10. This process will begin with the initial collection of factors influencing IoT systems, followed by expanding the list using the snowballing method. Subsequently, a panel of three experts will refine and validate these factors, culminating in the Delphi questionnaire to determine the final set of factors.

4- Evaluation And Results

Medical equipment plays a critical role in diagnosis, prevention, treatment, and patient care, with factories and companies worldwide engaged in their production and distribution. Given the rapid advancements in medical technology, the production and utilization of high-quality and precise IoT systems in the healthcare sector are of paramount importance. Identifying the factors influencing dependability becomes a crucial task.

The author commenced the study by compiling a comprehensive list of factors influencing IoT systems. Subsequently, utilizing the snowball sampling method, the list of factors affecting the evaluation parameters was expanded, involving a total of 18 experts. Following this, a three-member expert panel refined the factors affecting IoT systems and provided definitions for each parameter (see Table 4). Electronic questionnaires were then developed and distributed simultaneously to all participating experts. Once all experts provided their responses, the study progressed to the subsequent phase. Opinions and responses were anonymized and shared with all participants. After collecting responses and incorporating necessary revisions, the process underwent further review, and a revised questionnaire was distributed to the experts for consensus-building. This iterative process was repeated five times throughout the study.

Table 5: Factors Affecting Dependability in IoT Systems

Factor	Description	Reference
Standard	The use of multiple standards in the IoT can have a significant impact on improving the usability, efficiency, security, communication, and interoperability of different devices and systems, as well as reducing implementation costs while providing simplicity and efficiency in system development and implementation.	[28]
access level	Precisely defining user access levels helps mitigate security risks associated with unauthorized access to IoT devices. By defining appropriate access levels, individuals and users who should not have access to specific devices will be prevented from accessing them, thereby reducing security risks and unwanted intrusions.	[29]
protocol	Different protocols are used in the IoTs, each with its advantages and disadvantages. Proper utilization of protocols suitable for IoT systems can play a significant role. For example, using security protocols like TLS and SSL can enhance security in the IoT.	[30]
Training users	User education in areas such as security and protection of IoT devices can have a significant impact on optimizing the use of these devices and preventing potential harm.	[31]
Up-to-date device	Updating devices improves their performance and functionality, enabling the execution of new and advanced applications. It can also contribute to energy efficiency in device operation.	[32]
Network stability	The impact of network behavior and influential parameters on the stability of the IoT network is highly significant and crucial. Network stability is of utmost importance in certain domains such as healthcare and nuclear power.	[33,34]
Support	Due to the large number of diverse devices and their geographical spread, repairing and supporting them becomes challenging. Moreover, most IoT devices possess advanced capabilities and new technologies that require specialized expertise and experience for their maintenance and support.	[35]
Quality	The quality of IoT devices is highly important as it directly impacts the performance and efficiency of IoT systems. If quality is not ensured, it can lead to serious issues in the functionality of the system and the services provided by it.	[36]
Flexibility	IoT systems need to have the capability for future support and scalability. Given the complexity of IoT systems and the continuous changes in the industry, flexibility in these systems is highly important.	[30]
Monitoring	Monitoring in the IoT enables increased accuracy in the measurement and monitoring of various data, as well as predicting future decisions to prevent system errors. Additionally, by utilizing monitoring technologies in IoT, it is possible to reduce energy consumption and costs associated with the maintenance and support of these systems.	[37]
Management	Prognostics and systems health management is a field that utilizes sensors to evaluate the condition of systems, identify abnormal behavior, and forecast the remaining useful performance throughout the lifespan of the asset.	[38]

In the final stage, Fig. 2 identifies and categorizes the evaluation parameters and the influencing factors associated with them. For each evaluation parameter, the influential factors have been specified. Attention to these factors contributes to the improvement of the respective evaluation parameters, ultimately leading to the enhancement of the dependability of the IoT system. The explicitly outlined evaluation parameters, along with their corresponding factors, play a crucial and pivotal role in the production and development of IoT systems.

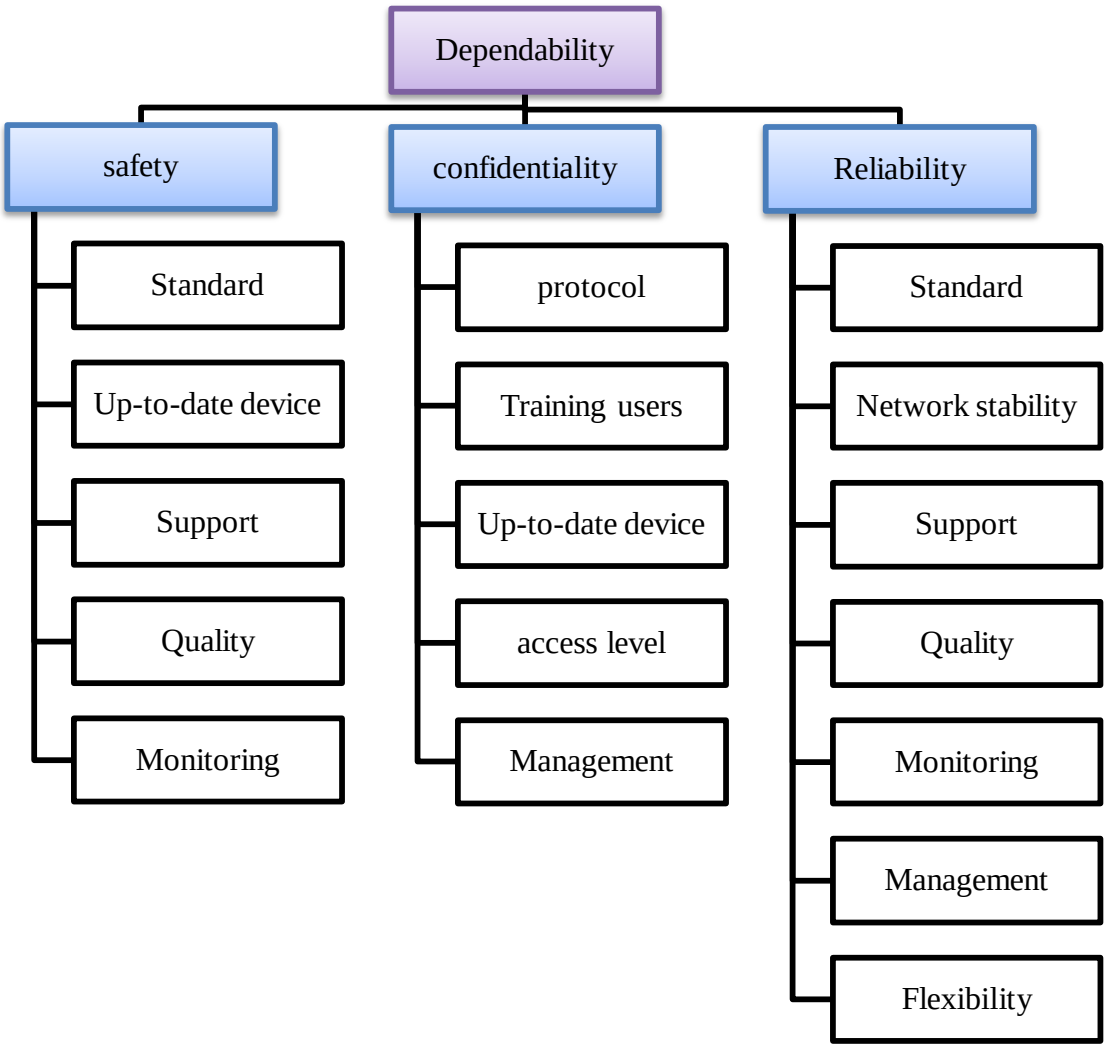

Figure 2: Parameters and Factors Affecting Evaluation Parameters

To assess the validity of the Delphi questionnaire, Cronbach's alpha coefficient was employed. Cronbach's alpha serves as a measure of internal consistency for measurement instruments, such as questionnaires or tests designed to evaluate various characteristics. It acts as a criterion for evaluating the validity of questionnaires and tests. This coefficient indicates the internal consistency of the questionnaire, disclosing the extent to which the items of a measurement instrument are interconnected and effectively measure a shared concept or property. Formula (1) for calculating Cronbach's alpha is as follows:

$$\alpha = \frac{k \,.\, S^2}{S^2 + (k-1) \,.\, \sigma^2} \tag{1}$$

where:

- j is the number of items (questions) in the questionnaire.
- S^2 is the variance of the mean scores of all items.
- σ^2 is the variance of the mean scores of each item.

Cronbach's alpha value falls within the range of 0 to 1, with a higher value indicating greater internal consistency and reliability of the questionnaire. As Cronbach's alpha approaches 1, the questionnaire is considered more reliable.

Cronbach's alpha is a dependable tool known for its properties of consistency and reproducibility. It can be applied in diverse contexts and consistently provides similar results across various applications. In this study, it is crucial to assess whether respondents consistently interpret the questions.

The acceptability or validity of a questionnaire refers to the reliability and accuracy of the information collected through that questionnaire. In other words, the validity of a questionnaire measures its ability to accurately measure the intended characteristics or concepts. In this article, Content Validity Ratio (CVR) and Content Validity Index (CVI) methods were used.

In the CVR method, experts provide a rating of 1 to 5 for each question in the questionnaire based on their experience and knowledge. The level of agreement among the experts regarding the ranking of each question is calculated. If more than 70% of the experts reach similar rankings for a question, that question is considered to have acceptable content validity. This means that the question has been appropriately included in the questionnaire and is consistent with the overall purpose of the questionnaire. The calculation is performed using formula (2), in which N represents the number of experts, and individuals denote essential cases.

$$CVR = \frac{Ne - \frac{N}{2}}{\frac{N}{2}} \quad (2)$$

where:

- Ne is the number of individuals who deemed the sample item (question in the questionnaire) as essential.
- N is the total number of individuals in the sample (all individuals who provided their opinions).

In the CVI method, experts assess the degree of relationship between each question in the questionnaire and the overall concept of the questionnaire based on an evaluation scale. This scale is created in the form of a simple table, where the overall concepts of the questionnaire are listed in the columns, and the questions of the questionnaire are listed in the rows. For each question, the experts assess its relationship with the overall concept of the questionnaire using a 4-point scale (very low, low, moderate, high).

In this method, if the agreement level among experts regarding the relevance of a question to the overall questionnaire concept exceeds 0.70 [39-43], that question is considered to have an acceptable content validity. In other words, a question is recognized as being in good alignment with the overall questionnaire objective. Formula (3) is employed to calculate it:

$$\text{CVI} = \frac{Nl}{N} \quad (3)$$

where:

- Nl is the number of acceptable items (items with an agreement level among experts regarding their relevance to the overall questionnaire concept exceeding 0.70).
- N is the number of experts.

In both CVR and CVI methods, using formulas (2) and (3), the level of agreement among experts in assessing the content validity of questions serves as a measure for evaluating the quality of content in questionnaires and measurement tools. This agreement is crucial for ensuring the validity and reliability of measurement instruments.

The statistical methods used in this article include the Snowball Sampling method, the Delphi technique, reliability analysis (Cronbach's alpha coefficient), and validity analysis (CVR and CVI). For calculations and data analysis, Excel 2022 and SPSS software were utilized. To facilitate the analysis of the influential factors, response values were assigned based on their level of association: unrelated (1), weakly associated (2), moderately associated (3), strongly associated (4), and highly associated (5).

If the number of raters is more than two, it is recommended to use the Intra-class

Correlation Coefficient (ICC) instead of Cohen's kappa coefficient for assessing agreement and reliability.

The results obtained from the questionnaire on factors affecting dependability are presented in Table 5. As you can see, the judges have provided similar opinions.

The results from CVR and CVI indicate that the questionnaire has good reliability in areas where the judges reached a consensus. All the important factors have a CVI value greater than 0.7, which is considered highly satisfactory.

Table 6: Factors Influencing the Parameters of Dependability, Safety, and Confidentiality

	Reliability		Safety		Confidentiality	
	CVR	CVI	CVR	CVI	CVR	CVI
Standard	1	1	1	1	0.6	0.066
access level	0.466	0	0.066	0.066	0.333	0.066
protocol	0.6	0.066	0.2	0.066	1	1
Training users	-0.2	0	0.333	0	1	1
Up-to-date device	0.6	0.066	1	1	1	1
Network stability	1	1	-0.06	0.066	-0.33	0
Support	1	1	1	1	0	0
Quality	1	1	1	1	-0.33	0.133
Flexibility	1	1	0.2	0.066	-0.2	0
Monitoring	1	1	1	1	0.333	0.2
Management	1	1	0.733	0	1	1

The Cronbach's alpha coefficient has been computed for each of the factors affecting the evaluation parameters of dependability, safety, and confidentiality. The obtained results can be observed in Table 6.

Table 7: Cronbach's Alpha Coefficients

	Reliability	Safety	Confidentiality
Cronbach's Alpha Coefficients	0.99	0.991	0.987

Continuing with the examination of the "Correlation Among Experts," each of the three Dependability parameters is addressed in Tables 7, 8, and 9. Each table is scrutinized separately for a detailed analysis.

1) Correlation Among Experts in the Reliability Parameter:

As depicted in Table 7, the Average Measures stand at 99%, signifying a substantial consensus among experts regarding factors influencing the Reliability parameter. This indicates a high level of agreement among professionals, emphasizing the significance of considering these influential factors during the production and development of IoT systems. The recommendation is to carefully incorporate these factors to enhance the

reliability of IoT systems during their manufacturing and development phases.

Table 8: Correlation Among Experts in the Reliability Parameter

	Intra-class Correlation	95% Confidence Interval		F Test with True Value .5			
		Lower Bound	Upper Bound	Value	df1	df2	Sig
Single Measures	.865	.784	.932	6.093	20	280	.000
Average Measures	.990	.982	.995	48.740	20	280	.000

Table 9: Correlation Among Experts in the Safety Parameter

	Intra-class Correlation	95% Confidence Interval		F Test with True Value .5			
		Lower Bound	Upper Bound	Value	df1	df2	Sig
Single Measures	.885	.813	.943	7.291	20	280	.000
Average Measures	.991	.985	.996	58.331	20	280	.000

Table 10: Correlation Among Experts in the Confidentiality Parameter

	Intra-class Correlation	95% Confidence Interval		F Test with True Value .5			
		Lower Bound	Upper Bound	Value	df1	df2	Sig
Single Measures	.833	.737	.914	4.730	20	280	.000
Average Measures	.987	.977	.994	37.841	20	280	.000

The column "95% Confidence Interval" straightforwardly represents the confidence intervals for Intra-class Correlation within the class. As depicted in Table 7, the upper and lower bounds of the Reliability evaluation parameter exceed 78%, which is an acceptable figure. This signifies excellent agreement among experts in the given context, indicating a high level of consensus among the professionals.

The F-test statistic has been calculated for the hypothesis:

H0: ICC = 0 vs H1: ICC > 0.5

For the Reliability parameter, the hypothesis examines whether the Intra-class Correlation Coefficient (ICC) is equal to zero or greater than 0.5. If the null hypothesis (ICC = 0) is accepted, it indicates a lack of agreement among judges, rendering the reliability of the study unacceptable. If the alternative hypothesis is confirmed, it suggests an acceptable level of reliability. The probability value (Sig) for each hypothesis is crucial. A value of 0.01 indicates rejection of the null hypothesis, signifying that the ICC is significantly greater than 0.5.

2) Correlation Among Experts in the Safety Parameter

As illustrated in Table 8, the Average Measures are at 99%, indicating a substantial consensus among experts regarding factors influencing the Safety parameter. This highlights a high level of agreement among professionals, underscoring the significance of considering these influential factors throughout the production and development process of IoT systems. It is recommended to meticulously incorporate these factors into

the IoT system production and development process to enhance the reliability of these systems during their manufacturing and development phases.

The column "95% Confidence Interval" straightforwardly presents the confidence intervals for the Intra-class Correlation within the class. As illustrated in Table 8, the upper and lower bounds of the Safety evaluation parameter surpass 81%, a figure deemed acceptable. This signifies outstanding consensus among experts in the specified context, denoting a high level of agreement among professionals.

The F-test statistic has been computed for the hypothesis testing scenario:

H0: ICC = 0 vs H1: ICC > 0.5

For the safety parameter, the hypothesis is designed to evaluate whether the Intra-class Correlation Coefficient (ICC) is equal to zero or exceeds 0.5. The acceptance of the null hypothesis (ICC = 0) suggests a lack of agreement among judges, leading to the conclusion that the study's reliability is deemed unacceptable. Conversely, the confirmation of the alternative hypothesis indicates an acceptable level of reliability. The significance level (Sig) associated with each hypothesis holds paramount importance. A Sig value of 0.01 signifies the rejection of the null hypothesis, indicating that the ICC is significantly greater than 0.5.

3) Correlation Among Experts in the Confidentiality Parameter

As depicted in Table 8, the Average Measures stand at 98%, signifying a significant consensus among experts concerning factors impacting the Confidentiality parameter. This underscores a high degree of agreement among professionals, emphasizing the importance of incorporating these influential factors throughout the production and development phases of IoT systems. It is advisable to conscientiously integrate these factors into the production and development processes of IoT systems to improve their reliability during the manufacturing and development phases.

The column "95% Confidence Interval" clearly depicts the confidence intervals for the Intra-class Correlation within the class. As demonstrated in Table 9, the upper and lower bounds of the Confidentiality evaluation parameter exceed 81%, a value considered acceptable. This indicates an exceptional consensus among experts in the defined context, signifying a high level of agreement among professionals.

The F-test statistic has been calculated for the hypothesis testing scenario:

H0: ICC = 0 vs H1: ICC > 0.5

For the Confidentiality parameter, the hypothesis is formulated to assess whether the Intra-class Correlation Coefficient (ICC) is equivalent to zero or surpasses 0.5. The acceptance of the null hypothesis (ICC = 0) implies a lack of consensus among judges, resulting in the determination that the study's reliability is considered unacceptable. Conversely, the affirmation of the alternative hypothesis suggests an acceptable level of

reliability. The significance level (Sig) associated with each hypothesis is of paramount significance. A Sig value of 0.01 indicates the rejection of the null hypothesis, signifying that the ICC is significantly greater than 0.5.

As mentioned, the factors affecting reliability were identified by experts using the proposed heuristic method. Questionnaires were used for this purpose, and their validity and reliability needed to be confirmed. The validity of a questionnaire refers to its conceptual and content accuracy and is an important criterion for assessing the quality of the questionnaire. The reliability of a questionnaire refers to the accuracy and stability of its results. In this section, it was demonstrated that the proposed method has high validity and reliability, and these factors affecting reliability can be used in the design and development of IoT systems in the healthcare domain.

5- Conclusion

In conclusion, this study employed a comprehensive approach to identify and categorize factors influencing the reliability, safety, and confidentiality of IoT systems in the healthcare domain. Integrating the snowball sampling method and the Delphi technique facilitated gathering expert opinions, refining influential factors, and categorizing them based on evaluation parameters. The findings of this research demonstrated the high validity and reliability of the methodology used. Experts achieved consensus on the critical factors affecting IoT system dependability, as evidenced by robust Cronbach's alpha coefficients and favorable validity assessments (CVR and CVI) of the questionnaire. These factors were systematically categorized, providing actionable insights for designing and developing dependable IoT systems in healthcare. This study contributes significantly to enhancing IoT system dependability in healthcare by addressing multifaceted challenges. As technology continues to advance, the insights gained here can guide manufacturers, designers, and policymakers in ensuring the reliability, safety, and confidentiality of medical IoT devices.

Looking ahead, future research should focus on several key areas to further advance the field of IoT system dependability in healthcare. Implementation and validation of the identified factors in real-world IoT systems, exploration of emerging technologies to enhance dependability, addressing regulatory compliance challenges, promoting interdisciplinary collaboration, and incorporating user-centered design principles are crucial steps. By addressing these areas, future research can build upon the foundation laid in this study, advancing the reliability and efficacy of IoT systems in healthcare.

References

1. Knight, J., Fundamentals of dependable computing for software engineers. 2012: CRC Press.

2. Whig, P., et al., Computational Science Role in Medical and Healthcare-Related Approach. Handbook of Computational Sciences: A Multi and Interdisciplinary Approach, 2023: p. 245-272.

3. Do Nascimento, I.J.B., et al., Infodemics and health misinformation: a systematic review of reviews. Bulletin of the World Health Organization, 2022. 100(9): p. 544.

4. Zhang, J., et al., Using usability heuristics to evaluate patient safety of medical devices. Journal of biomedical informatics, 2003. 36(1-2): p. 23-30.

5. Hasan, M.K., et al., A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications, 2022. 16(5): p. 421-432.

6. Silva, I., et al., A dependability evaluation tool for the Internet of Things. Computers & Electrical Engineering, 2013. 39(7): p. 2005-2018.

7. Macedo, D., L.A. Guedes, and I. Silva. A dependability evaluation for Internet of Things incorporating redundancy aspects. in Proceedings of the 11th IEEE international conference on networking, sensing and control. 2014. IEEE.

8. Bagula, A., O. Ajayi, and H. Maluleke, Cyber physical systems dependability using cps-iot monitoring. Sensors, 2021. 21(8): p. 2761.

9. Andrianto, H., et al., Performance evaluation of IoT-based service system for monitoring nutritional deficiencies in plants. Information Processing in Agriculture, 2021.

10. Airehrour, D., J. Gutierrez, and S.K. Ray. A lightweight trust design for IoT routing. in 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). 2016. IEEE.

11. Abdulhamid, A., et al. Dependability of the Internet of Things: Current Status and Challenges. in 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). 2022. IEEE.

12. Mehedi, S.T., et al., Dependable intrusion detection system for IoT: A deep transfer learning based approach. IEEE Transactions on Industrial Informatics, 2022. 19(1): p. 1006-1017.

13. Zhang, Y., et al., High-performance isolation computing technology for smart IoT healthcare in cloud environments. IEEE Internet of Things Journal, 2021. 8(23): p. 16872-16879.

14. Wu, H., M. Dyson, and K. Nazarpour, Internet of Things for beyond-the-laboratory prosthetics research. Philosophical Transactions of the Royal Society A, 2022. 380(2228): p. 20210005.

15. Khan, A.A., et al., QoS-ledger: Smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. Electronics, 2021. 10(24): p. 3083.

16. Uma, S. and R. Eswari, Accident prevention and safety assistance using IOT and machine learning. Journal of Reliable Intelligent Environments, 2022. 8(2): p. 79-103.

17. Khan, M., et al., Tag and IoT based safety hook monitoring for prevention of falls from height. Automation in Construction, 2022. 136: p. 104153.

18. Rafi, K., et al., Regulatory and standards development in medical additive manufacturing. MRS Bulletin, 2022. 47(1): p. 98-105.

19. Malvehy, J., et al., New regulation of medical devices in the EU: Impact in dermatology. Journal of the European Academy of Dermatology and Venereology, 2022. 36(3): p. 360-364.

20. Toscas, F.S., et al., Management of medical equipment in the Brazilian public health system (SUS), historical situation and the context of the pandemic COVID-19: a cut for lung ventilators. Health and Technology, 2023: p. 1-7.

21. Liu, Y., et al., Achieving privacy-preserving DSSE for intelligent IoT healthcare system. IEEE Transactions on Industrial Informatics, 2021. 18(3): p. 2010-2020.

22. Goodman, L.A., Snowball sampling. The annals of mathematical statistics, 1961: p. 148-170.

23. Nur, A.S. and E. Nurvitasari, Geometry skill analysis in problem solving reviewed from the difference of cognitive style students junior high school. Journal of Educational Science and Technology, 2017. 3(3): p. 204-210.

24. MOKHTARIANPOURZAVAREH, M., A. KHODAYARI, and M. KOHANDEL, Determining the components of the model of sustainable development of mountain tourism in Iran. Journal of Tourism and Development, 2022.

25. Diaz, J.M., L.A. Warner, and S.T. Webb, Outcome Framework for School Garden Program Development and Evaluation: A Delphi Approach. Journal of Agricultural Education, 2018. 59(2): p. 143-165.

26. Lei, L., et al., Construction of life-and-death education contents for the elderly: a Delphi study. BMC Public Health, 2022. 22(1): p. 802.

27. Varndell, W., M. Fry, and D. Elliott, Applying real-time Delphi methods: development of a pain management survey in emergency nursing. BMC nursing, 2021. 20(1): p. 1-11.

28. Abdel-Basset, M., G. Manogaran, and M. Mohamed, Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. Future Generation Computer Systems, 2018. 86(9): p. 614-628.

29. Ourad, A.Z., B. Belgacem, and K. Salah. Using blockchain for IOT access control and authentication management. in Internet of Things–ICIOT 2018: Third International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 3. 2018. Springer.

30. Lin, J., et al., A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal, 2017. 4(5): p. 1125-1142.

31. Davari, N., et al., Investigating the Effect of Information Security Awareness on Behavioral Intention to Use IoT Devices: A Case Study of Iran. Journal of Cyber Security Technology. 5(1): p. 47-62.

32. Kavak, H., et al., Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 2021. 7(1): p. tyab005.

33. Akkaş, M.A., R. Sokullu, and H.E. Çetin, Healthcare and patient monitoring using IoT. Internet of Things, 2020. 11: p. 100173.

34. Amini, M.R. and M.W. Baidas, GoodPut, collision probability and network stability of energy-harvesting cognitive-radio IoT networks. IEEE Transactions on Cognitive Communications and Networking, 2020. 6(4): p. 1283-1296.

35. Phuyal, S., D. Bista, and R. Bista, Challenges, opportunities and future directions of smart manufacturing: a state of art review. Sustainable Futures, 2020. 2: p. 100023.

36. Alhasan, A., et al., Quality of service mechanisms in internet of things: a comprehensive survey. Journal of Advanced Research in Dynamical and Control Systems, 2019. 11(2): p. 858-875.

37. Holey, S. and M.S. Bhosale, Smart health care system using internet of things. International Journal of Innovations in Engineering Research and Technology, 2016: p. 1-4.

38. Kwon, D., et al., IoT-based prognostics and systems health management for industrial applications. IEEE access, 2016. 4: p. 3659-3670.

39. Adetunji, O., et al., Patient-centered care and geriatric knowledge translation among healthcare providers in Vietnam: translation and validation of the patient-centered care measure. BMC health services research, 2023. 23(1): p. 1-11.

40. Cires-Drouet, R.S., et al., High prevalence of chronic venous disease among health care workers in the United States. Journal of Vascular Surgery: Venous and Lymphatic Disorders, 2020. 8(2): p. 224-230.

41. dos Santos Silva, G.W., et al., Content validity of an instrument for assessing healthcare needs of people with disabilities. International Archives of Medicine, 2016. 9.

42. Mao, X., A.Y. Loke, and X. Hu, Developing a tool for measuring the disaster resilience of healthcare rescuers: a modified Delphi study. Scandinavian journal of trauma, resuscitation and emergency medicine, 2020. 28: p. 1-12.

43. Wong, F.M., First data in the process of validating a tool to evaluate knowledge, attitude, and practice of healthcare providers in oral care of institutionalized elderly residents: content validity, reliability and pilot study. International journal of environmental research and public health, 2021. 18(8): p. 4145.