Internet of Things risks, benefits, challenges in industrial application: Survey

Ahmed Abdelmonem[*1], Shimaa S. Mohamed [2]

[1,2] Faculty of Computers and Informatics, Zagazig University, Zagazig, 44519 Ash Sharqia Governorate, Egypt
Emails: aabdelmounem@zu.edu.eg ; shimaa_said@zu.edu.eg

Abstract

The Internet of Things (IoT) is a crucial and rapidly developing technology that is employed in a wide variety of essential real-life apps, including those in which it may be used to enhance decision making. However, the presence of a number of potential sources of uncertainty inside the IoT infrastructure might influence decision makers to take decisions that are not suitable. In the work that is being presented here, the primary emphasis is placed on the development of a risk-based decision-making methodology for the Internet of Things (IoT), with the goal of efficiently managing uncertainties and incorporating prior domain knowledge into the decision-making process. The creation of the framework is based on a systematic literature analysis that examines the risks and reasons of ambiguity in decision-making systems related to the internet of things (IoT). IoT risk contains many and conflicting criteria so, the concept of multi-criteria decision making is introduced to overcome this problem. The purpose of this article is to provide the comprehension survey of the decision making based on IoT risk evaluation.

Keywords: Industrial Application; IoT; Risk; Big Data; Healthcare

1. Introduction

The term "Internet of Things" (IoT) represents a network that is comprised of all physical items (things) that are capable of interacting with one another and exchanging data via the use of machine-to-machine interactions. The Internet of Things (IoT) is the technology that makes it possible for numerous real-world apps, such as transportation, healthcare, energy conservation, and agricultural monitoring. In an Internet of Things configuration, a huge number of raw data are gathered from a variety of sensors, and they are then communicated for further analysis through short- and long-range communication technologies. This allows the data to be used in a variety of contexts. After the data have been processed, they are evaluated to determine the high-level environment and to infer important knowledge. This information may then be put to use by controllers to make crucial choices. Nevertheless, the presence of a number of different sources of ambiguity is a substantial obstacle that may have a considerable effect on the decision-making process in IoT systems. Uncertainty is a broad phrase that may be used to convey a variety of different ideas, including vagueness, confusion, and imperfection. In situations where Internet of Things (IoT) systems are linked with high-risk choices, the prevalence of ambiguity may drive decision makers to undertake improper actions that may have substantial repercussions. This is particularly true in scenarios when uncertainty leads to high-risk judgements. Uncertainties connected with data collecting, information processing, analysis techniques, and inadequate coverage of a given area are some of the causes of uncertainty in decision-making that is based on IoT[1], [2].

In IoT networks, these ambiguities may be brought on by the existence of restricted battery and computing capacity, high security needs, and other factors, amongst others. The heterogeneity, scalability, dynamism, and timeliness of an Internet of Things system all contribute to an increased

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

level of complexity inside the system; as a result, it is even more challenging to effectively manage uncertainty within the system. As a result, the risk evaluation-based IoT is a complicated multi-criteria decision-making (MCDM) process since there are several qualitative and quantitative variables to consider.

The usage of IoT has been quickly expanding due to significant applications in a variety of sectors. The Internet of Things presents several possibilities to various businesses as a result of its capacity to gather, communicate/share, and analyse data. Tracking and monitoring that is allowed by the Internet of Things, for instance, may increase the efficiency of manufacturing and the distribution of final products. The Internet of Things provides various novel solutions, including the development of new business models, in addition to the enhancement of operational efficiencies. With the use of data created by Internet of Things devices and connection in real time, for instance, sales of products might be supplemented with associated services. Tzeng proposed a framework that places an emphasis on delivering business value through the refinement of business processes and the expansion of the business model in the hope that it will encourage more organisations to adopt RFID technology. This was done in order to assess the business value of RFID system. Nevertheless, the adoption of IoT in large-scale industrial applications confronts a number of obstacles. The primary problems are (1) Energy efficiency; (2) Interaction and information difficulties (connectivity, latency, throughput, standards); (3) Expandability (net size, compatibility); and (4) Protection and stability concerns (reliability, privacy protection).

Various systems of the Internet of Things (IoT) technologies, such as sensor devices, back-end systems, and designs for Service-Oriented Architecture (SOA), all share a number of these difficulties. Applications of the Internet of Things have already achieved a level of success that is considered to be satisfactory in a number of sectors, including the healthcare services sector, the food supply chain (FSC), and the infrastructure monitoring sector.

2. Related Work of the IoT and Industrial Application

In a variety of real-world contexts, the Internet of Things functions as a technology that makes it possible to improve both situational awareness and the quality of decisions. Researchers have highlighted ambiguity as one of the primary constraints that restrict the implementation of IoT technology to enhance decision-making. This uncertainty may be found in both the material realm and in the system itself. In the context of making decisions in supply chain based on IoT data, the quality of the data has also been recognised as an important component. It has been stated in the research that intercommunication alone are not sufficient for Internet of Things systems to be able to make intelligent judgements. Cognitive Internet of Things refers to the idea that "things" connected to the internet should have the capacity to learn, think, and comprehend.

The Internet of Things (IoT) has a lot of potential since it will link millions of different things that people use on a daily basis so that they can offer them with intelligent and pervasive services. The quantity of data that is created as a result of this deployment on a worldwide basis is enormous. In order to deliver Internet of Things services, the collected data will be used as a foundation upon which to derive insights on individuals, things, and phenomena. The accuracy of the data is one of the primary concerns raised by this situation. In point of fact, the dependability of data is very necessary for the engagement of users and the general adoption of the IoT paradigm.

Karkouch et al. [3] conducted a study on data quality (DQ) with regard to the Internet of Things. In the context of the Internet of Things, they identified data attributes and their new lifecycles. The notion of data quality (DQ) is explained, and then a collection of general and domain-specific DQ characteristics that are appropriate for use in evaluating IoT data is chosen. There is an ongoing investigation of the Internet of Things-related issues that threaten the data's quality. In addition, a comprehensive qualitative examination of their influence on a variety of DQ characteristics, and therefore on the total DQ, is offered here. In addition, they found important DQ difficulties' manifestation forms such data outliers and discrepancies in data from several sources, among other things, and they correlated every presentation class with its manifestations in relation to the impacted DQ dimensions.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

The current trend demonstrates that data semantics in the internet of things has developed into an important component of everyday life. It offers opportunities for the interaction and exchange of specialised information. Ontology modelling shines out a lot in providing semantics with the defined description formats, which provide a remarkable capacity to mix and share information from a variety of sources. This makes it a wonderful choice. Shi et al. [4] made a definition of data semantics in the Internet of Things (IoT), covering related ideas, generic architectures, essential methodologies, applications, and problems. It is true that ontology modelling has become the most widespread approach up to this point, and that these techniques have been presented. These techniques are engaged in data semantization. Ontologies have high expressivity, expansibility, and the capacity for deductive reasoning, and they may be used to describe any entity, any context, any user, and any behaviour. In their study, a broad overview of data semantics is presented, as well as a comparison of several ontology models and automation tools. In the last part of the report, the problems and outstanding concerns that have been identified throughout the survey are discussed. These topics include standardisation and generalisation, intricacy and dynamic nature, as well as privacy and safety. This is an important field that will have a significant impact on industry in the years to come.

It is not unreasonable to suppose that human-centric systems have a significant impact on the lives of the individuals who use them. The intense usage of HCNs, on the other hand, results in a massive volume of newly created data traffic, which uses up a substantial number of DCN resources in terms of of their processing capability, storage capacity, and energy consumption. Nevertheless, these data provide the raw product from which significant information is obtained in order to be employed by new applications that are known to be disruptive. Alzate-Mejía et al. [5] presented a pretty thorough review of judgement computational modeling such as multicriteria decision making (MCDM), particle swarm optimization, and machine learning. These computational methods have been proposed to be used in a variety of application domains, including telephony, health insurance, logistics and transportation business and consider a company, and company's production planning, amongst others. It has been shown that every single one of the suggested procedures has the potential to be significantly hampered by the uncertainty that is present in the retrieved data, which has the potential to distort the information that is gained from them. Dealing with uncertainty is very challenging due to the wide variety of factors that contribute to it, which include anything from external interference to human behaviour. It is abundantly clear that a new paradigm for transdisciplinary computational analysis has to be established in order to evaluate and deal with uncertainty concerns. Because of the implications and repercussions of making incorrect use of highly confidential, technological, and commercial information, protecting one's data and maintaining one's privacy are of the utmost significance and should be given careful consideration. In order to safeguard society in all of its facets, there is an urgent need to place a significant amount of attention on the promotion of the formation of governance norms to avoid the exploitation of sensitive data. If this doesn't change, the HCN will quickly lose its credibility and will never be recognised or embraced by anybody. A closer examination of such developing ideas as Intelligent Spaces or Industry 4.0 reveals a concerning lack of globally accepted benchmarks, even at the level of the idea meanings. This absence of standards may put the connectivity of devices, as well as single- and bridge apps, at risk. Table 1 shows the previous works concerned with IoT risks.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

Table 1: The previous works concerned with IoT risks

Author	Application	Main Idea	Drawbacks
Hussain et al.[6]	Healthcare application	In spite of the fact that there are many different kinds of uncertainty, their in-depth analysis of the relevant study revealed that Internet of Things (IoT) technologies may be used for trustworthy decision making. The results of the examination of the relevant literature have been analysed, consolidated, and provided in the form of a risk-based methodology for strategic planning in IoT systems. Managing the underlying causes of ambiguity in IoT systems throughout the process of data analytics and subsequently combining technical knowledge with ML results is the primary emphasis of this specific piece of research. After that, we will be able to make use of action rules as a suggestion and decision assistance tool. It was also found that the well-calibrated CRF approach not only helps with the measurement of uncertainty in the forecasts that an ML model makes, but it also offers a natural way to integrate that uncertainty with domain knowledge. This was another finding that was made. As a consequence of this, the incorporation of domain information, like the environment of an action, allows us to recognise the actual activity that was carried out via the use of a thresholding technique. In addition, if an action has been projected to take place at a level that is below the limit, it may be described using language that is intelligible to humans. After then, the person responsible for making the choice might use the boost customer in order to calculate the cost that is linked with a decision. In addition to this, it was discovered that the results of the machine learning algorithm may be encoded with a wealth of contextual information, which can turn a risk into an opportunity. It was discovered that the IF-THEN action rules that were presented were helpful for providing semantics to the predictions. This is something that is often needed in intelligent omnipresent apps such as HAR.	Small dataset
Zakaria et al.[7]	Healthcare application	The goals of the Internet of Things in healthcare, which are to expand access to medical care, enhance the level of care provided, and lower the overall cost of medical treatment. This may be accomplished via the development of an IoT Security Risk Management Model for Healthcare Practice that is both effective and safe. COBIT 5 will give a standard set of acknowledged principles, methods, tools, and models to assist in increasing the value and confidence that all care workers have in one another. The desire of the enterprise's management staff to invest in Internet of Things technology is an essential component in assuring the efficacy of the adoption. The higher the level of IoT implementation by doctors and professionals, the higher the degree of understanding among the medical fraternity in the institution, and the proper going to support IT infrastructure become possible causes of successful or swift and seamless implementation of cloud computing for the health industry.	Their model not evaluated by the IoT experts
Thibaud et al.[8]	Healthy and safety industries	They gave a thorough analysis of publications on high-risk EHS businesses from the viewpoint of the Internet of Things (IoT). It is essential, in light of the explosion of IoT-based apps and the relevance of high-risk EHS businesses, to take stock of the studies and findings that have already been obtained and to identify any gaps that need to be filled in order to make progress. The mining and energy businesses (oil and gas and nuclear), navigation systems, and building and power grid management with an emphasis on disaster response operational processes are the specific focuses of our research. Other areas of interest include the healthcare services sector, the forest products sector, the mining industry, and the nuclear energy industry. They spoke about the reasons why there is already research being done on Internet of Things-based solutions in high-risk EHS businesses. The special features of IoT-based apps in various sectors, including architectural design, sensor layer, connectivity, back-end system, and business elements, were then brought to light by our team. Concerning the difficulties associated with the Internet of Things in high-risk EHS sectors, we have seen that the present study focuses more on the technological difficulties than it does on the social and economic considerations. Because of this approach, solutions are developed that address technological difficulties first. The issues and trends of future research are going to be quite similar: it seems that the primary attention will be directed to technological challenges and developments, particularly in terms of communication and processing capacity.	not address the gap that exists between conceptual frameworks and practical applications on a wide scale.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

3. IoT Applications and Risk in Mining and Energy

In the mining and energy (oil and gas, and nuclear) sectors, the prevalence of IoT-related technologies in research and in commercial applications may be attributed to a number of variables, including the following: A) There are a big number of professionals who are directly or indirectly engaged in the production process; B) There are a large number of manufacturing and maintenance facilities that are spread out throughout the country; C) A large variety of processes and procedures that could result in a diverse range of scenarios (for example, transmission lines could be under water, underground, or above the ground or in extreme environments such as salt water, hillside, or desert); D) The development of cloud computing for oil exploration and the increasing interest in it; E) A number of safety problems (for example, harm to the environment or loss of life), such as the bursting oil pipeline in Michigan (United States of America) in 2010 that went undiscovered for 17 hours or the possibility of radioactive materials being released; F) Inaccurate data collection as a result of manual control procedures and approximate estimation (for example, in oil wells, everyday production is calculated based on collected with the help liquid); G) A lack of centralized data network platforms, which results in large amounts of data that are disconnected from one another. Table 2 shows the application in IoT risks.

Table 2: IoT risks in various application.

Application	System architecture	Market	Communication
Healthcare	Architecture with the traditional three layers	Broad consumer market demand Apps based on the Internet of Things that have a greater intrinsic worth but a longer projected return on investment	Putting regulatory and industry norms under restraints
Food supply chain	Centralized, Linear, and Distributed Architectures, with Distributed Architecture Receiving the Most Attention From Researchers	Applications that are associated to the Internet of Things have a low maturity level owing to the high complexity of the FSC.	No specified communication standards Using a mix of centralised and peer-to-peer routing in a distributed architecture is an example of a hybrid routing strategy. A significant amount of the mobile communication system that is available worldwide in order to handle the widespread placement of sensors Due to the challenging environment, a combination of wireless and cable connection is used.
Mining and energies	The significance of being informed of the circumstance and having assistance for making decisions	There is a significant potential for advances in competitiveness, but improved decision-making assistance is required.	Multiple modes of communication (including vehicle-to-vehicle and vehicle-to-infrastructure communications, among others)
Connected vehicles	Solutions that are centralised vs those that are decentralised	Strong potential for market growth, Existing research reveals a multitude of X-as-a-Service business concepts.	The difficulty of high mobility: varying topology and a large number of barriers in the surrounding area hinder communications. The current solutions are not scalable due to spectrum shortages, security concerns, the expense of deploying massive amounts of infrastructure, etc.
Infrastructure management	A centralised approach that places an emphasis on real-time capabilities	Put your attention on the deployment of various apps to pave the way for a fruitful development process.	Combining limited and unconstrained modern communications: balancing the need for dependable and high-quality data transmission with the need to save as much electricity as possible

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

4. Benefits of IoT

The data that is generated by IoT is the primary factor that determines the effect that its adoption has on enterprises. The Internet of Things consists of three components: "Big," "Open," and "Linked" (BOLD). To begin, the Internet of Things (IoT) produces voluminous amounts of data that are, on average, of higher quality than data produced by more conventional methods. This is due to the IoT's higher level of detail and, consequently, its often greater accuracy; its greater heterogeneity, which results from its originating from a greater variety of sources; its greater timeliness, which results from its frequently being real-time or very close to it; and its substantially larger volumes. As a result, the data generated by IoT devices are sometimes referred to as "Big" data because of its volume, diversity, and velocity. Big Data, which is created by IoT, does, however, come with certain hazards attached to it. These risks are often linked with the administration of the data and the constraints of IT infrastructure. Second, since the Internet of Things is an open platform, data that was originally gathered for a specific purpose may be repurposed for use in a variety of applications in order to accomplish a number of different objectives and uncover previously unknown insights. However, this open nature may also provide issues, for instance in the area of security. The third advantage of the Internet of Things is that it enables enterprises to mix data from a variety of sources, including data from "things" as well as data that is more conventional. On the other hand, this interconnected element may also provide issues, such as those concerning individuals' right to privacy[9], [9].

The melded integration of multiple devices and communication solutions, like detection and tracking innovations, wired and wireless sensor and pneumatic cylinder networks, enhanced protocols, and dispersed intelligence for intelligent devices, RFID, Digital Product Code new tech, and ZigBee technology, is an important factor that enables the adoption of the Internet of Things. The Internet of Things is heterogeneous, which means that, for instance, many different kinds of sensors from numerous sources may be utilised to enable public safety and adherence to rules. This might provide methods of control that are possibly more effective than old approaches. As a result, analytics performed on large amounts of data have the potential to play an essential part in enabling wise governance and facilitating cooperation amongst agencies working together[10]–[12].

According to Chui and colleagues' findings, having adequate data from networked devices facilitates better decision-making and allows for superior analysis in terms of monitoring or situational awareness. Apps for the Internet of Things not only make it possible to collect data in a more effective manner, but they also make it possible to capture fresh data with a finer level of granularity on tasks and activities. As according Rathore, Ahmad, Paul, and Thikshaja, the intelligent management of the traffic system, along with the provision of factual facts to the citizen according to the current traffic problem, has a significant impact on the life of the citizen and improves the efficiency of the Cosmopolitan authorities. Additionally, this kind of control has the potential to significantly improve the quality of life in the metropolitan area. In their study, Rathore et al. mention that the Internet of Things (IoT) generates large amounts of data, and that decreasing the random deviation of mean in data gathering might lead to an increase in the amount of faith that can be placed in the findings. According to Kwon, Lee, and Shin's findings, the implementation of big data may have a significant impact on the data quality. As a result, the increased timeliness and sheer amounts of data offered by IoT have the potential to improve the performance of companies by enhancing their capacity for planning process and the speed with which they can respond to occurrences that were previously unanticipated. In addition, particularly in the field of asset management, IoT is becoming an increasingly popular tool for monitoring the quality and health of organisational assets[13]–[15].

IoT applications are primarily seen as being able to automate the process of data collection, as stated by Boos et al. These applications eliminate the need for human involvement in the process of data capture. The Internet of Things (IoT) generates large amounts of data that can be shared publicly for anybody to utilise. Making information and records accessible to the public may increase the transparency of a company, which in turn can assist improve business processes and save waste. Via greater access to information, empowering people and businesses may be accomplished through enabling customer self-service through the Internet of Things.

IoT enables organisations to supervise what is taking place in the real world at actual, growth and expansion leeway and service efficiency, allowing for better decision making, and often going to lead to new sources of revenue. Haller et al. Subirana believe that the company value can be inferred from IoT by enhancing real-world visibility, and by decomposing business processes. This is because IoT

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

enables organisations to monitor what is taking place in the real world at real-time. The potential of the Internet of Things to inform and automate may, in the long run, ultimately lead to a revolution of the traditional business procedures that are in place[16].

According to Bi et al., the connected component of the Internet of Things (IoT) has the potential to lower labour costs and increase public empowerment by allowing customer self-service. One example of this would be self-service check-out lanes in grocery stores. The data that was collected as a consequence may be pooled, which then leads to knowledge into product demand. These insights enable supermarkets increase the quality of their assortment, which in turn improves consumer pleasure. Fleisch is of the opinion that the ability of IoT to connect data from several sources implies that it may facilitate the identification of fraud, which in turn can reduce expenses associated with fraud and increase customer confidence. In addition, the insights that are obtained via the linkage of data from multiple sources enable for enterprises to engage with their customers in a more efficient manner, which opens up new chances for communication and helps support extra service revenues[12], [13].

According to the findings of Hashem and colleagues, efficient analysis and usage of big data are crucial components of success in a variety of commercial and service fields. This entails the capability of Internet of Things equipment and technology to gather information about process management in a cost-effective and efficient manner without the need for time-consuming physical counts. This is done so that insights gleaned from processed information and evaluation can be used to increase efficiency, performance, and compliance[14], [15].

5. IoT Risk in Various Applications

A lot of academics believe that sensitive information, like lifestyle style or individual economic information, might be revealed as a result of data breaches, which could have a significant and negative influence on individuals' right to privacy. It is crucial, for this reason, to protect this data from being accessed in an inappropriate manner and by unauthorised parties, while at the same time allowing authorised users to see created data. As a result, while Big Data may provide us with the data we require to be able to discover faced with new insights, the juxtaposition of IoT can be discovered in the adjustments to organisations that are required in order to to transform Big Data into usable while protecting the rights of the person. As a result, while Big Data may provide us with the data we require to be able to uncover response to emerging observations, the juxtaposition of IoT can be found in the changes to organisations that are necessary to be Although it is often assumed that big data would increase the quality of the information the truthfulness and speed of big data may render it more difficult to analyse the data[17]–[19].

Because of the duality of IoT, changes that take place in staff and organisational processes may in turn lead to additional changes in the IT infrastructure. This can happen as staff members get more aware of the opportunities presented by Big Data and as new needs become accessible. According to Dwivedi and colleagues, there is no one infrastructure that has been demonstrated or is the best, and the quality of the data is sometimes ambiguous and has to be explored. As a consequence of this, unanticipated risks may also involve technological difficulties such as restrictions in the capabilities of the information technology (IT) infrastructure.

The mitigation of these risks often results in unanticipated expenses, one of which is a lower return on investment. Because it might be expensive to create an Internet of Things system that is completely functioning in its whole, high prices can be seen as a key barrier to the widespread adoption of IoT.

Many people believe that it should be possible for consumers to make use of items that other individuals have got to share and to end up making use of objects in their own apps, maybe in ways that the owner of the thing had not anticipated. This is related to the fact that allowing others to connect and use the stuff that have been accepted for publication publicly on the Internet is a key facilitator of the Internet of Things (IoT), as was previously discussed. Thus according Zuiderwijk and Janssen, the majority of the previously conducted study on the "openness" of data has focused on data supply as its primary focus. On the other hand, because of the dual nature of the openness offered by the Internet of Things (IoT), it is necessary to have a developed system of processes in order to broadcast and

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

share things, as well as to guarantee that they can be located and accessed. As an example, Qian and Che cite search localization, scalability, and real-time processing as significant obstacles to the deployment of IoT. Thus according Qian and Che, the current methods of searching are predicated on the exchange of information through a distant connection, and thus often fall short in their ability to properly enable local searches of physical items[20]–[22].

Because of the requirement to continually monitor a large variety of objects while also adapting to a wide range of contexts, there are a number of technical and regulatory hurdles that need to be overcome. Data ownership, information security, and information exchange are often mentioned as being among the most difficult technological and legislative concerns. However, new security concerns are becoming more and more apparent, and there are only a few solutions that are persuasive enough to provide fine-grained access control for Internet of Things applications, particularly those that are sensitive.

According to Zeng et al., it is not unusual for Internet of Things (IoT) systems to be integrated with preexisting apps in both a direct and indirect manner. As an illustration, RFIDs are frequently integrated in an indirect manner through an RFID reader and in a direct manner through an engrained server. The technology behind the Internet of Things may have a very diverse set of rules and abilities, among other things. While we have seen that some studies argued that the advantages of data individual differences, the juxtaposition is that the diversity at the component level can also be a major hindrance to IoT implementation due to compatibility issues. This is because variability at the component level can lead to a lack of compatibility between devices. In addition, customers of data are often diverse as well, and various applications may use a variety of processing techniques for the data that they use. Thus according Zeng and colleagues, the heterogeneity of the Internet of Things makes it particularly difficult to build designs for the Internet of Things. This is emphasised by Qian and Che's findings, which show that searching in IoT needs a technique of architectural design of browsers. This is due to the fact that developing an adequate search engine for IoT is not a simple task. This might imply that whilst integrating IoT data can give advantages, a lack of regulations and implementation standards can also severely hamper the adoption of IoT[7], [23].

The incorporation of IoT into a business model necessitates the development of new expertise, as well as new organisational structures and operational procedures. For instance, owing to skill worker shortages as well as a lack of available educational and training opportunities, locating and hiring suitable individuals may be an extremely difficult task. Many studies are also of the opinion that a resistance to change or an unwillingness to learn about new technology is a common trait in many businesses[24]. Figure 1 shows the framework for risk management.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

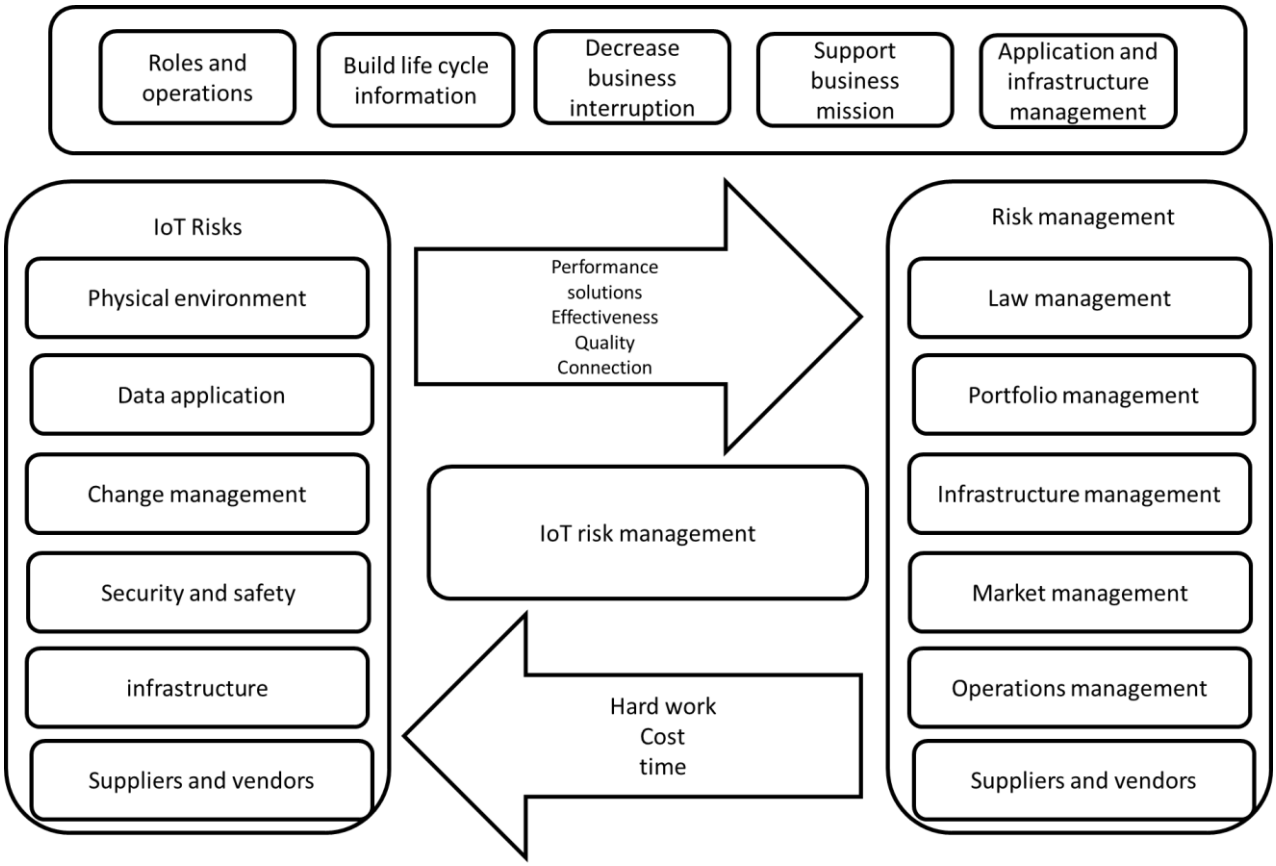

Figure 1:The framework of risk management.

6. IoT Challenges

The below are some of the technological problems associated with IoT: A) Scaling (net size, interoperable); B) Energy - efficient; C) Telecommunication and data-related difficulties (internet access, delay, bandwidth, standards); D) Security and confidentiality (reliability, privacy protection)[5], [25]–[28].

According to the research that has been done so far, the following are some of the most pressing social and economic problems: A) The business model B) The standardisation In the field of healthcare, for example, researchers have established a number of unique protocols specifically for wearable technology without taking into consideration the possibility of compatibility with other systems. E) Affordability versus high cost of implementation F) Absence of global or national regulations and standards G) Duration for IoT-based apps[29]–[34]. Table 3 shows the IoT challenges.

Table 3: The IoT challenges.

Technical	Effective use of energy, Challenges relating to both communication and data collection (connectivity, latency, throughput, standardization), Scalability (network size, interoperability) (network size, interoperability), Protection and safeguarding (reliability, privacy protection)
Social and Economics	Business model, Standardization, Conformity with applicable regulatory requirements and industry standards, Commitment and understanding from the many parties involved, including assistance

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

	for local communities and training for staff members. Credibility among all parties involved, including customers (trust and social acceptance), Comparing the low cost of implementation with the high cost of implementation, Due to the absence of international or national regulations and standards, Time-to-market, Unoccupied Space Political issues (responsibility, consensus between stakeholders)

7. Finding

ITU–Internet T's of Things reference model is a standardised four-layer design that makes it easier to deploy IoT for individual systems and use cases. This architecture was developed by ITU–T. As a result, we have mapped the components of the IoT-DM to the standardised reference architecture that is provided by the ITU–T in order to make interoperability easier to achieve, as well as to make development simpler and easier. As can be seen in Figure 2, the ITU–T conceptual framework is made up of four high-level layers in addition to two levels that are related with each of these four layers.

Hussain et al. utilised a case study in a Smart Home setting with the emphasis on assessing the performance of the suggested CRF model inside the IoT-DM framework by utilising the open-source benchmark dataset. This evaluation was done in order to determine whether or not the model was effective.

For the purpose of comparing and evaluating the IoT-DM framework's overall performance, a conventional action system for diabetes has been taken into consideration. During the course of their research, it was discovered that the model had incorrectly diagnosed the resident as having symptoms of diabetes for a period of three days with an accuracy of 83.4%. This was done in the context of the diabetic use case. For instance, the suggested model mistakenly labelled the "eating" action as "idle," and as a consequence of this labelling error, 17.6 percent of cases of sadness were incorrectly diagnosed for the user. This conventional framework does not have the capacity to determine the explanation behind incorrectly labelled cases of diabetes activity. Even while the framework makes it possible to automate activities, there is no way to choose the instances of a task that can be relied upon. In addition, operators deal with raw output and are consequently unable to grasp the behaviour of a model, which is required in order to take crucial decisions. Due to the fact that the conventional framework does not have any of the aforementioned skills, the medical expert will be led astray into taking activities that are not suitable since there is no mechanism to recognise risk inside the decision-making process. On the other hand, the risk-based architecture for the Internet of Things that was suggested includes numerous criteria to prevent taking improper actions for a diabetic use case that is comparable.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

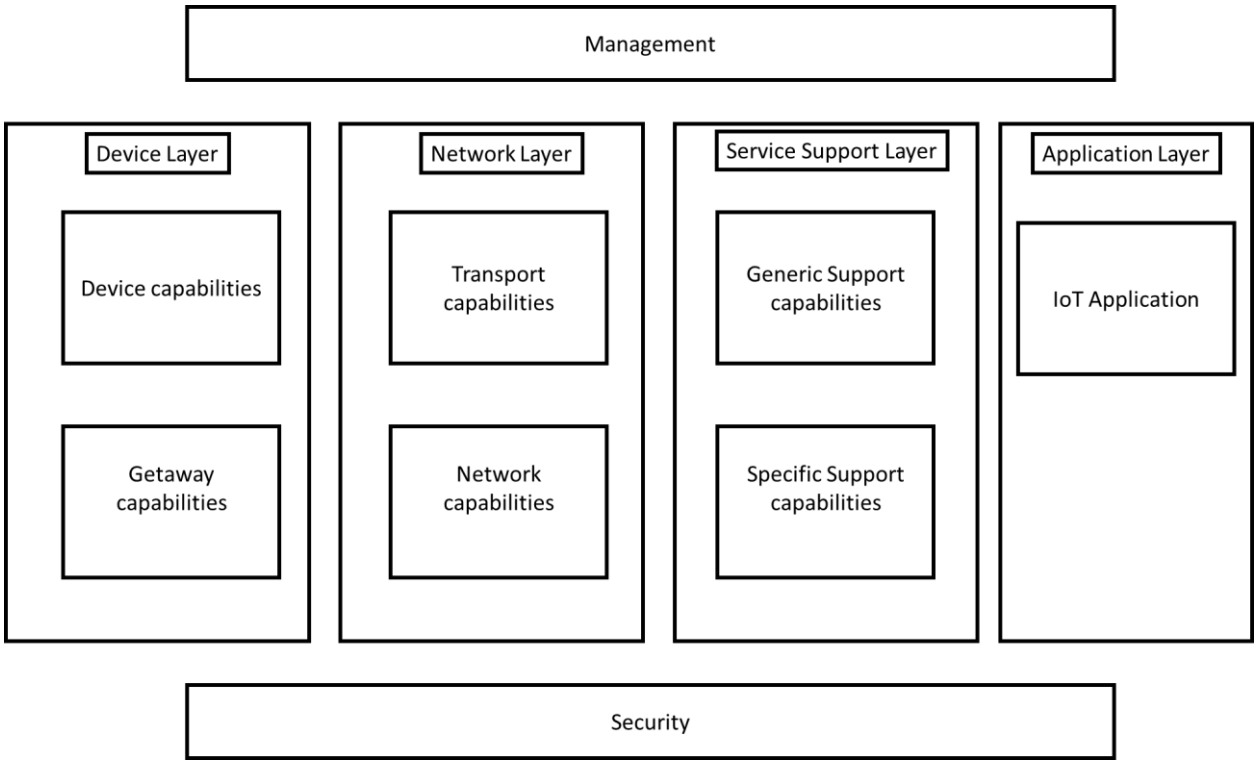

Figure 2: Conceptual framework IoT

8. Conclusion

The use of the tech is a result of human behaviours, and these actions decide the real benefits that may be derived from the Internet of Things (IoT), despite the fact that IoT gives a number of advantages. This study presents a comprehensive analysis of the possible advantages and threats of the Internet of Things (IoT), as well as insight into the dualism of IoT in two different scenarios.

From the point of view of the Internet of Things, we presented a complete summary of previous research on high-risk sectors. In light of the meteoric rise in the number of IoT-based applications and the growing importance of high-risk sectors, it is essential to conduct a comprehensive review of previous research and findings and to identify any gaps in knowledge that need filling.

References

[1] S. Madakam, V. Lake, V. Lake, and V. Lake, "Internet of Things (IoT): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[2] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," *International journal of computer applications*, vol. 113, no. 1, pp. 1–7, 2015.

[3] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "Data quality in internet of things: A state-of-the-art survey," *Journal of Network and Computer Applications*, vol. 73, pp. 57–81, 2016.

[4] F. Shi, Q. Li, T. Zhu, and H. Ning, "A survey of data semantization in internet of things," *Sensors*, vol. 18, no. 1, p. 313, 2018.

[5] N. Alzate-Mejía, G. Santos-Boada, and J. R. de Almeida-Amazonas, "Decision-making under uncertainty for the deployment of future hyperconnected networks: A survey," *Sensors*, vol. 21, no. 11, p. 3791, 2021.

[6] T. Hussain, C. Nugent, A. Moore, J. Liu, and A. Beard, "A Risk-Based IoT Decision-Making Framework Based on Literature Review with Human Activity Recognition Case Studies," *Sensors*, vol. 21, no. 13, p. 4504, 2021.

[7] H. Zakaria, N. A. A. Bakar, N. H. Hassan, and S. Yaacob, "IoT security risk management model for secured practice in healthcare environment," *Procedia Computer Science*, vol. 161, pp. 1241–1248, 2019.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

[8] M. Thibaud, H. Chi, W. Zhou, and S. Piramuthu, "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review," *Decision Support Systems*, vol. 108, pp. 79–95, 2018.
[9] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. H. D. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges," *IEEE Internet of things Journal*, vol. 5, no. 5, pp. 3758–3773, 2018.
[10] F. Nausheen and S. H. Begum, "Healthcare IoT: benefits, vulnerabilities and solutions," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 517–522.
[11] R. De Michele and M. Furini, "Iot healthcare: Benefits, issues and challenges," in *Proceedings of the 5th EAI international conference on smart objects and technologies for social good*, 2019, pp. 160–164.
[12] A. Banafa, "IoT and blockchain convergence: benefits and challenges," *IEEE Internet of Things*, vol. 9, 2017.
[13] R. Gupta and R. Gupta, "ABC of Internet of Things: Advancements, benefits, challenges, enablers and facilities of IoT," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016, pp. 1–5.
[14] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, 2018.
[15] M. S. Jalali, J. P. Kaiser, M. Siegel, and S. Madnick, "The internet of things promises new benefits and risks: a systematic analysis of adoption dynamics of IoT products," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 39–48, 2019.
[16] N. N. Dlamini and K. Johnston, "The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review," in *2016 international conference on advances in computing and communication engineering (ICACCE)*, 2016, pp. 430–436.
[17] P. Brous, M. Janssen, and P. Herder, "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*, vol. 51, p. 101952, 2020.
[18] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," 2018.
[19] I. Cvitić and M. Vujić, "CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT.," *Annals of DAAAM & Proceedings*, vol. 26, no. 1, 2015.
[20] K. Boeckl *et al.*, *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. US Department of Commerce, National Institute of Standards and Technology …, 2019.
[21] W. Xi and L. Ling, "Research on IoT privacy security risks," in *2016 International Conference on Industrial Informatics-Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII)*, 2016, pp. 259–262.
[22] F. I. Salih, N. A. A. Bakar, N. H. Hassan, F. Yahya, N. Kama, and J. Shah, "IOT security risk management model for healthcare industry," *Malaysian Journal of Computer Science*, pp. 131–144, 2019.
[23] P. Radanliev, D. C. De Roure, C. Maple, J. R. C. Nurse, R. Nicolescu, and U. Ani, "Cyber Risk in IoT Systems," 2019.
[24] V. Malik and S. Singh, "Cloud, big data & IoT: risk management," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 2019, pp. 258–262.
[25] R. Van Kranenburg and A. Bassi, "IoT challenges," *Communications in Mobile Computing*, vol. 1, no. 1, pp. 1–5, 2012.
[26] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.
[27] H. S. Birkel and E. Hartmann, "Impact of IoT challenges and risks for SCM," *Supply Chain Management: An International Journal*, 2019.
[28] E. P. Yadav, E. A. Mittal, and H. Yadav, "IoT: Challenges and issues in indian perspective," in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2018, pp. 1–5.
[29] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*, 2014, pp. 230–234.
[30] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business horizons*, vol. 58, no. 4, pp. 431–440, 2015.
[31] S. Balaji, K. Nathani, and R. Santhakumar, "IoT technology, applications and challenges: a contemporary survey," *Wireless personal communications*, vol. 108, no. 1, pp. 363–388, 2019.
[32] C. C. Sobin, "A survey on architecture, protocols and challenges in IoT," *Wireless Personal*

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022

Communications, vol. 112, no. 3, pp. 1383–1429, 2020.
[33] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.
[34] S. G. H. Soumyalatha, "Study of IoT: understanding IoT architecture, applications, issues and challenges," in *1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications*, 2016, vol. 478.

DOI: https://doi.org/10.54216/AJBOR.080105
Received: May 07, 2022 Accepted: December 17, 2022