Journal of
Sensor and Actuator Networks

MDPI

Review

Socio-Organisational Challenges and Impacts of IoT: A Review in Healthcare and Banking

Tahera Kalsoom [1], Naeem Ramzan [2], Shehzad Ahmed [3], Nadeem Anjum [4], Ghazanfar Ali Safdar [5,*] and Masood Ur Rehman [6]

[1] Manchester Fashion Institute, Manchester Metropolitan University, Manchester M15 6BJ, UK; t.kalsoom@mmu.ac.uk
[2] School of Computing, Engineering and Physical Sciences, University of the West of Scotland, Paisley PA1 2BE, UK; naeem.ramzan@uws.ac.uk
[3] Higher Colleges of Technology, Abu Dhabi Women's Campus, Abu Dhabi P.O. Box 25026, United Arab Emirates; sahmed3@hct.ac.ae
[4] Department of Software Engineering, Capital University of Science and Technology, Islamabad 44000, Pakistan; nadeem.anjum@cust.edu.pk
[5] School of Computer Science and Technology, University of Bedfordshire, Luton LU1 3JU, UK
[6] James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK; masood.urrehman@glasgow.ac.uk
* Correspondence: ghazanfar.safdar@beds.ac.uk

Abstract: The Internet of Things (IoT) is transforming how organisations and individuals connect and interact with digital ecosystems, especially in sectors like healthcare and banking. While technological benefits have been widely discussed, the societal and organisational impacts of IoT adoption remain underexplored. This study aims to address this gap by conducting a systematic literature review (SLR) of 110 peer-reviewed publications from 2012 to 2024 across four major academic databases. The review identifies and categorises the key applications of IoT, its social and organisational drivers, and the challenges of its implementation within the healthcare and banking sectors. The analysis reveals that critical barriers to IoT adoption include security, privacy, interoperability, and legal compliance, alongside concerns around workforce displacement and trust. This study also introduces the 5Cs framework—connectivity, continuity, compliance, coexistence, and cybersecurity—as a practical lens for addressing these challenges. The findings highlight the need for responsible IoT integration that balances innovation with ethical, social, and organisational accountability. Implications of this research inform policymakers, practitioners, and researchers on how to design human-centric and socially sustainable IoT strategies in sensitive sectors.

Keywords: IoT; healthcare; banking; automation; user interaction; social impacts; organisational challenges

Academic Editor: Lei Shu

Received: 28 February 2025
Revised: 11 April 2025
Accepted: 14 April 2025
Published: 24 April 2025

Citation: Kalsoom, T.; Ramzan, N.; Ahmed, S.; Anjum, N.; Safdar, G.A.; Ur Rehman, M. Socio-Organisational Challenges and Impacts of IoT: A Review in Healthcare and Banking. *J. Sens. Actuator Netw.* **2025**, *14*, 46. https://doi.org/10.3390/jsan14030046

1. Introduction

The Internet of Things (IoT) interprets the connection of devices to the internet using embedded software and sensors to transmit, gather, and exchange data with one another, reducing human interaction [1]. Following years of hype, anticipation, and steady growth, IoT appears to be set to cross over into widespread commercial use. The percentage of firms that adopt IoT technologies has risen from 13% in 2014 to over 25% by 2021 [2]. In addition, the enterprise IoT market is anticipated to rise at a compound annual growth rate (CAGR) of 13% from 2023 to 2033, reaching USD 2021.9 billion by 2033 [3]. The

evolving technologies that underpin IoT are both a result and a motivation for this degree of adoption. For starters, technological advancements will make IoT easier to implement, allowing a wider range of businesses to profit from IoT applications. With continuously evolving advanced nanotechnology, the concept of connecting new and old technologies in the form of innovation and economic growth, the digital world seems to have collided with the physical world [4]. This has created numerous opportunities for businesses, however, with lingering challenges as well. Though IoT is shaping the lives of people and organisations, IoT's impact on society technologically, economically, and socially cannot be ignored. Technology and society are intertwined and analysing the advantages of one as a standalone case cannot reflect the whole picture [5].

Today's world is greatly moved by IoT, which connects every aspect of human life. The importance of IoT is worth emphasizing as it has a lasting and boundless impact on every individual's way of life. IoT applications range from communication to smart cities, security to healthcare, agriculture to industrial manufacturing, banking to sports, and education to governance [6]. Advancements in the Internet of Vehicles (IoV) have introduced route planning, video compression, and augmented reality (AR) navigation within vehicles that aim to enhance travel comfort [7,8]. In the post-pandemic world, technology companies have seen sharp growth resulting in a more visible impact of IoT on our lives [9]. Thus, IoT is reinventing our physical world by creating and supporting opportunities that were impossible before. Advancements in 5G, one of the key enablers of IoT due to high speed, massive bandwidth, low latency, and enhanced scalability have further driven the upsurge in IoT expansion. The possibilities offered by IoT are unlimited and most of the time they are beneficial [10]. Most of the research on the Internet of Things (IoT) is often overly optimistic because it tends to focus on the potential benefits of the technology and overlook the challenges and limitations. This overly optimistic view of IoT in much of the research is a result of a combination of factors, including the hype cycle, industry influence, lack of data, and focus on benefits. It is important for researchers and policymakers to consider both the potential benefits and the challenges of IoT in order to have a more realistic and nuanced understanding of the technology and its impact. At the same time, IoT has many societal impacts on top of the technical challenges as the world we see is connected and communicated through devices so small that they can fit in the palm of one's hand. The social impact of the Internet of Things (IoT) is a burning issue because it touches on a wide range of important societal concerns. Issues such as privacy and security, job displacement, inequality, addiction, and dependence on technology are important and require careful consideration and discussion. As more and more devices become connected to the internet, it is crucial that we understand the potential consequences of this technology and take steps to mitigate any negative effects. Unlike the internet, which has a well-documented design, architecture, and infrastructure, IoT is considered to be an extension of the internet, although it lacks global coherence. This raises issues primarily related to data security and privacy, creating implicit assumptions that data will be shared among things, applications, and possibly sectors [11,12]. Some researchers [13–17] state the perks of IoT include enhanced productivity, increased energy and transport efficiency, and greater control and auditing in manufacturing and supply processes, with a likeliness of increasing value by billions to the global economy. However, others [7,18–20] argue that there needs to be a balance of these benefits with both known and unknown risks to the privacy, security, and flexibility of users. In addition, unknown consequences may arise from the continuously increasing volume of data and energy produced and consumed by many different sources of IoT [21].

Exclusive challenges in research posed by IoT are becoming a source of fascination to researchers. Huge amounts of literature can be found discussing the infrastructure of IoT

including deployment and management of IoT systems. In the literature, a wide range of reviews on the advantages and benefits of IoT in everyday lives has predominated since the inception of this technology [22–24], while implications of increasing integration of IoT devices in society are rather neglected [9,25–28]. As indicated in [29–31], rare collections of pragmatic hints relating social impact of IoT were found that lack a stable foundation in the research community. A wide spectrum of literature can be found on the types of wireless sensor networks (WSNs) [32] and cloud computing [26,33] used to interconnect the physical world with information technologies [34–36]. However, after intensive research of the literature, it was found that the maintenance of these sensors and IoT devices gained little attention, especially in IoT research and development in the UK. The existing literature on the societal impact of IoT either discusses data privacy and security issues vaguely or provides recommendations on addressing these issues for future research. Moreover, the vulnerability of IoT devices by hackers has been feared but failed to attract the attention of the researchers, as very limited literature was found on this topic.

Most of the published articles deal with IoT benefits for organisations and the general public, with surveys about the accuracy of technological interaction with the physical world. Publications specifically devoted to social aspects such as number of jobs created as a result of induction of IoT technology, quality of jobs (safe, sustainable, and skilled) [22,37], types of beneficiaries available to customers (affordability, accessibility, and ease of use) [38,39], financial profits [40,41], quality of life, and environmental effects of heavy energy usage [26,40,42] are rare. Terms such as big data, technological strategy, innovation, operational performance, government policies, and rules and regulations were found in the majority of the publications. Fewer papers look into knowledge management, the value of un-monetised environmental effects, data monetisation, and asset utilisation by organisations implementing IoT technology rapidly. In addition, few publications addressed security, data privacy, and legal issues arising as a result of cybercrime of IoT technology. Only a small number of research papers were found dealing with human-centric IoT, which discussed the human and social side of IoT; however, these were completely devoid of human behavioural studies.

Surveys on IoT computing platforms and industrial IoT solutions have been constantly conducted since the early 2000s [2,16,30,43,44], including context-aware communications and applications [45,46]. However, the result of this extensive literature study shows that no study has focused on the quality of experience of the interaction of customers with IoT devices in the UK. Questionnaires on IoT implementation status and benefits are regularly organised [32,34,47,48], but those related to labour demand/productivity, customer experience, use of technology, and asset utilisation by UK customers have not been considered yet. The majority of the respondents are owners, facilitators, and providers of IoT technology [49–51], rather than the general public. Nevertheless, attracting the huge interest of researchers on technological advances and technical challenges [2,14,52,53], IoT has received minimal attention on its social impacts [5,10,54–56]. In addition, although IoT devices connect machines to humans, the human-centricity of IoT devices is lacking in the current studies.

Moreover, the organisational impacts of IoT are important to analyse because IoT has the potential to significantly transform how organisations operate, interact with customers, and generate revenue. The widespread adoption of IoT technology has significant implications for organisations, as it has the potential to revolutionise the way they operate, interact with customers, and deliver products and services. For instance, IoT technologies can help organisations automate and streamline their operations, leading to improved efficiency and cost savings. This can result in better profitability, higher productivity, and competitive advantage. In addition, IoT technologies can help organisations to better understand their

customers' needs and behaviours, leading to more personalised and effective customer experiences. This can result in increased customer satisfaction, loyalty, and retention, which are the main goals of the healthcare and banking sectors. While IoT can bring many benefits to organisations, there are also potential negative impacts that should be considered. IoT technologies can add complexity to organisational systems, requiring specialised expertise to design, integrate, and manage. This can increase costs and create operational challenges. Moreover, IoT devices may not be compatible with existing infrastructure or legacy systems, requiring significant investment in new technology to make them work effectively. In addition, IoT devices can replace human workers, leading to job displacement or requiring workers to develop new skills to adapt to the new technology. Therefore, it is very important to study not only the societal impact of IoT but organisational challenges as well, as they are both linked to human behaviour. In this regard, this research provides a unique perspective on IoT-related investigations in the healthcare and banking sectors. It will help researchers and practitioners realise the importance of human behaviour in adopting IoT and devising effective solutions to these issues in these two important fields.

In order to carry out this research, answers to three research questions are explored to unearth the reasons for the main question under investigation. Firstly, key applications of IoT in the healthcare and banking sectors are analysed, and then the social and organisational drivers of IoT implementation in these sectors are probed followed by an inquest of the social and organisational challenges posed by IoT technologies within these two sectors.

Contributions of This Study

The predicted huge effect of IoT in terms of re-shaping our lives, something as vast as a change to society, necessitates characterisation of its social impacts. The intent of this paper is to cover the knowledge gap between vast benefits and huge promises made by IoT on technological as well as economic fronts and its influence on redefining our societal and social behaviours by systematically reviewing the literature published in recent years. Since the social impacts of technology cannot be discussed without focusing on its usage, this study tends to provide the reader with a comprehensive account and holistic approach to the working framework, uses, key challenges, and social impacts of IoT and highlights potential new directions in the key fields of healthcare and banking, which is, to the best of our knowledge, a first of its kind.

The choice of healthcare and banking sectors as a case study is based on several reasons. Firstly, the healthcare and banking sectors are two of the most important user-oriented applications of IoT. Secondly, they are the leading sectors that have successfully adopted IoT into their daily operations and together play a crucial role in the economy of a country. Thirdly, as these sectors are public-centric with a wide range of customer interactions, the social impact of IoT becomes more visible and vital to assess. Fourthly, healthcare is a sector that widely uses IoT at an extensive level, whereas the banking sector is particularly new to IoT. Therefore, it is aimed to carry out a comparison of the best IoT adopters with the worst IoT adopters. In addition, an intensive literature search has been carried out to cover the theoretical and empirical literature identifying the use and advantages/disadvantages of IoT devices in the UK. Although the economic, environmental and societal impacts of IoT are equally large for both developed and developing nations around the globe, some countries are significantly investing in innovation and implementation of IoT technologies into their businesses and have much-improved infrastructure for IoT deployment. Looking into the IoT market of one of these countries can be more insightful. Hence, this work studies the IoT implementation in the UK as a case study, which is a front-runner in adopting IoT as a key pillar of its digital economy. Following the introduction in this

section, Section 2 discusses the development and implementation of IoT technology in the healthcare and banking sectors. Section 3 details the research methodology adopted for this work followed by the results of the systematic literature review and bibliometric analysis. Section 4 provides an in-depth overview of the social and organisational impact of IoT. Lessons learned are summarised in Section 5. Future research directions are discussed in Section 6 and conclusions are drawn in Section 7.

2. IoT in Healthcare and Banking

2.1. e-Healthcare

Healthcare is one of the leading sectors that has successfully adopted IoT into its daily operations. In healthcare services, IoT is primarily used to access information promptly. Healthcare service is a continuously progressive process that involves maintaining or improving the health of humans by diagnosing, preventing, and treating diseases. It not only includes activities within the hospitals but also those outside of hospitals, such as providing medical equipment and processing insurance documents [42,57]. Advancements in IoT technologies within healthcare have been given a term known as the Internet of Medical Things (IoMT) [9] and have created immense possibilities for providing high-quality and more convenient healthcare services. IoMT combines medical equipment with IoT devices, therefore providing sensing and processing capabilities to this equipment [9]. Healthcare providers use IoT in a variety of operations such as embedded context prediction, embedded gateway configuration, indirect emergency treatment, semantic medical access, wearable device access, and adverse drug reactions [20,58]. Wearable and implantable sensor devices such as digital pills, smart food, smart beds, and smart aids have been the focal point of IoT development in the healthcare industry [14,19]. A huge number of portable devices that can detect medical conditions by measuring pulse rate, alcohol level, blood pressure, body temperature, electrocardiography (ECG), electroencephalography (EEG), electromyography (EMG), and so on, are nowadays available for use [59]. Wound assessment has become a lot easier with an IoT-based wound assessment system [60]. IoT-based smartphone biosensors have the potential to detect various kinds of viruses including COVID-19 [61]. By adopting these technologies, employees in healthcare services (doctors, nurses, etc.) are able to make emergency medical decisions and reduce costs by having easy and instant access to different kinds of data resources online [33]. Voice-activated IoT devices are also able to provide urgent medical care [62]. Doctors are now able to access data to gain knowledge about the disease history and medicine-taking history of their patients. In addition, medicines are now bar-coded so that drugs can be delivered directly to patients. Ambulances are connected to global positioning systems (GPSs) and radio frequency identification (RFID) so that patients can be reached speedily [63–69]. A common e-health scenario is presented in Figure 1.

Access to health information through the implementation of IoT devices has raised some challenges as well. Ubiquitous access to data; physical storage, availability, and maintenance of huge amounts of data; energy usage; interoperability of different resources; privacy, security, and data anonymity; and unified and universal access are a few challenges to mention here [14,29,70–78]. The cloud computing concept is found to be useful to deal with most of these issues at the cost of energy consumption [79]. The diversity of IoT devices can also cause heterogeneity problems in the data format in IoT platforms. A lack of coordination in the e-health field can raise risks in the form of field workers becoming burdened with too many different devices running various different programs and software [33,80]. Also, high-quality healthcare cannot be delivered just by IoT devices, without sufficient numbers of healthcare professionals who are duly trained in using these devices and interpreting the data [81,82]. Society's acceptance of IoT in healthcare is wide

and increasing but knowledge management and awareness remain bounded to those customers who are tech savvy, whereas older generations are less adept the modern IoMT devices and require proper training to be able to monitor themselves through them [37,42,50,76]. The health sector could save huge costs if IoT is properly adopted [29,39,48]. However, a focused and strategically prioritised approach from all stakeholders along with substantial research and development efforts, proper training of the health professionals, and standardisation of vastly different IoT devices is the key to truly benefit from these advantages [23,83].

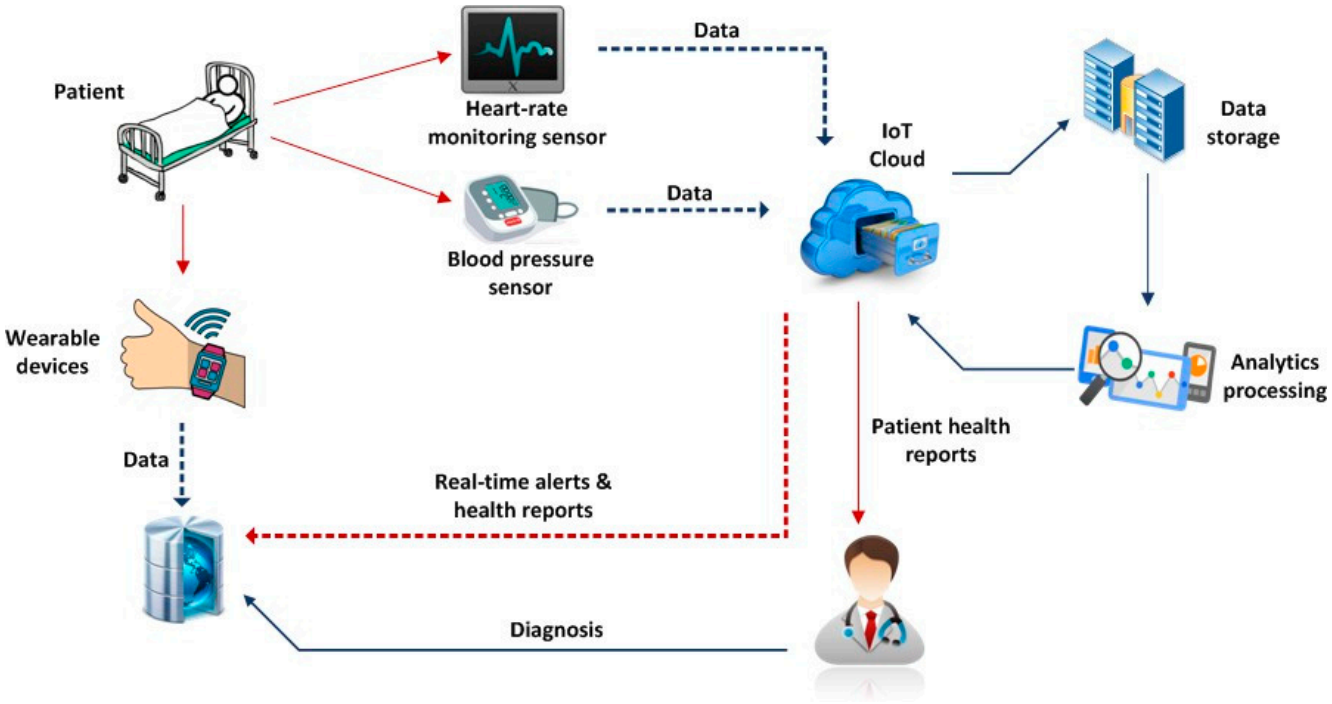

Figure 1. A typical e-healthcare scenario.

Different types of IoT technologies adopted and successfully used in modern healthcare systems are summarised in Table 1. Since healthcare is one of the major sectors employing IoT devices with access to very personal and sensitive information, it leads to substantial social insecurities. It is, therefore, pertinent to assess the social impact of healthcare.

Table 1. IoT technologies used in healthcare.

Technologies	Description	Refs.
Big data	• Today the use of big data seems to be one of the best techniques to capture, store, and analyse the data of patients. This interoperability may lead to inequality in access to data of value to individuals and communities from IoT. • In medicine, data were stored traditionally in hard copy, which requires extra cost. • Big data have an excellent capability to store data in digital form. • Big data maintain all patient data and billing system and clinical records. • Data are stored systematically, which quickly provides the best solution to healthcare.	[65–68]

Table 1. *Cont.*

Technologies	Description	Refs.
Cloud computing	• By using computer system resources, it provides on-demand data storage and describes data with the help of the internet. • It quickly shares patient information in urgent cases. • Shares proprietary data resources, which help doctors and surgeons to perform their jobs efficiently and effectively. • It increases data quality and reduces the cost of data storage.	[14,16,69,70]
Smart sensors	• It monitors and controls all parameters regarding patient health. • Easily monitors blood pressure, temperature, oxygen concentration, etc., of patients. • Helpful to obtain information on health status, defective bone, and surrounding biological tissue.	[38,52,68,71]
Software	• There is customised software available for the medical field that improves patient care, stores patient data, and gives treatment, associated tests, and diagnoses. • Helps to improve communication between patients and doctors. • Stores the medical history of patients, and confidential details and diseases of patients are easily identified and managed by the software.	[9,36,38,71,72]
Artificial intelligence	• Artificial intelligence helps to perform, evaluate, validate, predict, and analyse data in a predefined environment. • Provides excellent capabilities to predict and control infections and diseases. • With the help of this technology, doctors and surgeons achieve improved efficiency, accuracy, and effectiveness. • It measures the pain of patients with changes in medication.	[22,53,62,73,74]
Virtual reality/augmented reality	• The better way to integrate humans with electronic systems is to provide real-time information. • Virtual reality helps to improve the quality of planning, patient safety, and efficiency of patient treatment. • Provide needful information to patients and doctors to improve surgical planning quality. • Augmented reality also provides digital information of life in digital imagery/sound form.	[42,44,54,75]

2.2. e-Banking

IoT has not only changed the field of healthcare, but it has also brought a revolution in the finance industry that is gaining momentum through successful implementations of IoT in its development line. IoT has not only impacted the current practices and future expectations in the finance industry, it is also posed to dictate the future practices in the insurance and banking sector [48,84]. Today, banks are examining opportunities in which they can use big data to transform their relationships with customers [34,42]. The use of Blockchain in the banking sector is another frontier [85]. These developments led some researchers to the invention of a new term: "Banks of Things" [34,35,42,45,48]. In this new world of banking, with high integration of IoT at its core, the banks will act as customers' data protectors to manage and control privacy and sharing of the data, an advisory body between customers and sellers, and managers of customer payments [37,86]. Recent developments in mobile banking have not limited the banking business potential to just processing transactions; banks distribute value by offering multiple services via diverse payment channels such as point of sale, contactless, wearables, biometric chips, smart kiosks, and smart ATMs [87]. Customers can use smart devices to access data, which when accessed by banks, allows the banks to anticipate the needs of customers [42]. This can make the banks help customers with their smart financial decisions. As a result, the banks create customer loyalty, bringing in more business for them. A simple e-banking scenario is shown in Figure 2.

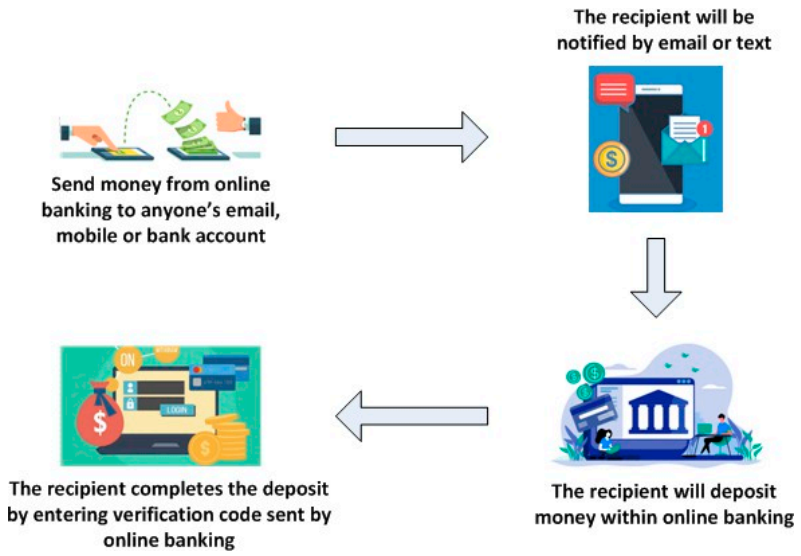

Figure 2. A typical e-banking scenario.

Digital channels can wear away the bond between customers and banks by reducing barriers to entry, therefore promoting switching behaviours and reducing human connection with the banks [88]. In addition to meeting customers' financial needs by providing them with loans and helping them manage their accounts, these consultancy roles of the banks will face a new dimension with IoT in meeting the non-financial needs of customers [48]. With a banker having access to collect data from a customer's fridge, electrical counters, or travel vehicles, banks can monitor and forecast the budget status of the customer. Therefore, banks can not only forecast certain expenses that might occur in the customer's budget, but they can also give the customer some preventive advice. Moreover, with access to more information about commercial customers, banks will have the ability to analyse and compare the supply and production chains, the dynamics about whom they compete, and the distribution networks of end products to customer preferences [48,51]. So, modern banks will differ from traditional banks in the way that they will no longer require commercial customers to submit their financial statements at the end of each period to analyse their banking practices. Some of the technologies of IoT used in banks successfully are mentioned in Table 2.

Table 2. IoT technologies used in banking.

Technologies	Description	Refs.
Mobile banking	• Mobile banking has been the newest addition established by micro-finance banks in both developed and developing countries. • Internet banking requires using a computer or a PC with an effective internet connection. • Application-based mobile banking has become a norm in the industry and is being provided by a majority of banks worldwide. • These applications are a reliable channel and allow users to carry out complex transactions, customise the interface, and also brand it accordingly.	[40,48,85,89]
Digital wallet	• A system or a service that promotes secure storage of users' payment credentials and passwords, enabling them to make payments through numerous online methods or a smartphone. • Customers are able to purchase items easily and quickly without worrying about forgetting their passwords. • Not only do individual customers benefit from using digital wallets, but companies also have a huge potential to increase their marketing opportunities by collecting consumer data. • Apple Pay, PayPal, and Google are examples of worldwide accepted and most-used types of digital wallets.	[89–91]

Table 2. *Cont.*

Technologies	Description	Refs.
Bank-in-a-box	• The bank-in-a-box is a solution provided by the banks that enables the transformation of core banking services such as payment solutions, deposit and loan products, internet and mobile banking, etc., to licensed application software through non-digital channels. • It reduces the costs of entry due to multiple banks sharing the same platforms and charges being made on the basis of a number of transactions and accounts. • By adopting preconfigured systems instead of developing their own, users have the ability to reduce the time it takes to enter the market. • With a stable platform with continuous updates, uncertainty is reduced for users as bank authorisation requests are more straightforward compared to unknown platforms.	[14,55,86,87]

2.3. Social IoT (SIoT)

Social IoT, as part of IoT, necessitates human beings and the regulations that govern society for optimal function and content development [92]. SIoT is a system that can receive the information it requires from the environment, and it is a critical factor in transaction accuracy and speed. Three important elements must be considered for every item placed in this system:

- Object ID Management: Each object has an identifier with which it is identified throughout the IoT system.
- Object Profiling: This contains static and dynamic information from each object in the network that acts as profiling information for other objects.
- Owner Control: This is a set of rules by object owners to control the behaviour of objects, such as how the objects communicate with each other, start, end, or change the state of themselves in the network.

After identifying objects, their owners grant authorisation for each object to be present and active in the SIoT system. The owner control is in charge of granting permissions that have a significant impact on how objects behave, such as establishing the maximum number of members and the criteria under which objects can create, terminate, or change their status [20,58]. As owners of objects, humans play a critical and important role in the formation and management of SIoT systems, as well as in ensuring their efficiency and efficacy.

The social Internet of Things (IoT) has the potential to bring about significant benefits to both the healthcare and banking industries, but there are also several challenges and concerns that need to be considered. In the healthcare industry, the use of social IoT has the potential to significantly improve patient outcomes, increase efficiency, and reduce costs. For example, remote patient monitoring, enhanced telemedicine, and improved communication between patients, healthcare providers, and caregivers can all result in better patient outcomes and improved quality of care. However, there are also privacy and security concerns that need to be addressed, as the collection and storage of sensitive personal health information raises significant concerns about data privacy and security. Project Nightingale is a very good example of such an issue raised as a result of patient data stored on IoT devices. Project Nightingale—a partnership between Google and Ascension—aims to bring Google's advanced data analytics to improve how information is used for patient care. Through this partnership, Google gained access to over 50 million Ascension patient's medical records. However, doubts have been raised regarding the security of the initiative and concerned individuals have questioned what precautions have been put in place to protect patients. In addition, people are upset by the inability to refuse involvement if they do not want their information shared.

In the banking industry, the use of social IoT has the potential to improve customer experience, increase efficiency, and reduce costs. For example, personalised services, real-time account updates, and improved risk management can all result in a better customer experience and improved financial outcomes. However, there are also security concerns that need to be addressed, as the use of IoT devices for financial transactions and data collection raises significant concerns about the security of financial information and the risk of fraud.

In both the healthcare and banking industries, it is important to consider the impact of social IoT on privacy and security and to take appropriate measures to mitigate these risks. This can include implementing robust security protocols, using encryption to protect sensitive information, and ensuring that data are stored securely. Additionally, it is important to consider the potential impact of social IoT on mental health and well-being and to take appropriate measures to minimise any negative consequences. While social IoT has the potential to bring about significant benefits to the healthcare and banking industries, it is important to critically evaluate its impact and take appropriate measures to mitigate potential risks.

1. *Trust:* IoT is a rapidly growing paradigm that includes a significant range of technologies that are predicted to usher in the next information revolution. However, according to a Packard study [93], more than 70% of present IoT systems have major vulnerabilities due to unsecured web interfaces, lack of transport encryption, insufficient permission, and inadequate software protection [84]. All of these new potential hazards to data protection and information security must be thoroughly considered as failures of IoT and may have dramatic consequences on the lives of people who depend on it, making them hesitant to adopt it widely [94].

In today's technologies, such as IoT and cloud computing, which deal with how objects interact together [93,95], trust is one of the most important topics. Due to a lack of trust in items that interact socially, issues such as loss of privacy, safety, security, access, and information tampering by unauthorised people or things arise [12,78]. Furthermore, object owners may carry out destructive assaults such as badmouthing, self-promotion, and on-off attacks based on their interactions with other objects; thus, measuring trust between them is critical for IoT to determine the optimum relationship between customers and suppliers [37]. Anything that needs to make a secure connection must have a high level of trust in the other items that want to connect. It can provide a greater level of trustworthiness communication for some requests and differentiate harmful and trustworthy items on the network.

Two types of trust between objects are presented by [96]: *Quality of service trust* (whether a device can prepare high-quality service in response to a requested service or not, and many other metrics including reliability and cooperativeness to evaluate QoS trust) and *social trust* (which is more customary in social IoT and is a level of trust between the owners of different objects that is evaluated by some factors like honesty and connectivity [96]).

Because it is widely dispersed and based on qualitative data, trust is essential in the IoT ecosystem [53]. The term "trust" is used in a variety of ways and in various settings. Despite the fact that trust is a critical topic that has received widespread attention, it is a difficult notion with no clear consensus in the scientific literature [89]. Trust is described in a range of potential meanings in information and communication technology (ICT) and is regarded as a fundamental characteristic of digital interactions by integrating trust in computers and humans [36]. The Internet of Things is no exception, as security is inextricably linked to consumers' capacity to trust their surroundings.

The level of confidence that an entity may provide to other entities for certain services in a specific situation is also known as trust [42]. Although trust is typically associated with humans, it may also refer to a device or any system, emphasising the need to assess the

level of trust in a digital community. As a result, trust in IoT is built on three levels: user to device, device to device, and device to user [20,58]. As a result, trust can be divided into three categories: entity trust, machine trust, and data trust. The need to communicate with dependable devices such as actuators and sensors is referred to as machine trust [11]. In the IoT world, this is an issue because it is not always possible.

Furthermore, because each entity evaluates confidence in any device differently, IoT systems must deal with non-singular perspectives on trust. The expected conduct of users or services is indicated by the IoT entity trust. Although dependable computing can help to build device trust, mapping such approaches to device trust is more difficult and exploratory. To develop device trust, practical approaches such as reliable computing for standardised devices and computational trust are required [11].

2. *Elements of Trust:* As the number of IoT-connected devices grows, so does the amount of communications, transactions, and data [44]. As a result, in order to remain fully functioning, trust systems must scale with the expanding number of devices. As a result, scalability requires the development of enforcement mechanisms, and new approaches must be evaluated based on their capacity to deal with a rising number of items in the network [38].

Infrastructure is also a challenge in terms of availability and locating other entities with which to communicate. Because entities require others to obtain information and interact with them, trust and reputation systems should consider this difficulty [14]. As a result, new systems and techniques must be evaluated in terms of their effectiveness.

Identity management is also an important aspect of IoT, as are trust and reputation systems. The fact that the identity of things is not the same as the underlying mechanism, that things can have a basic identity and many different identities, and that these things can also hide their true identity are all important components of this challenge [1,11,18,59].

Furthermore, ensuring that trust requirements are met is intertwined with access control and identity management [11]. This is a critical issue since the IoT environment is defined by a variety of devices that must process and manipulate data in accordance with user wants and rights. Controlling the status of the virtual world should be supported. Users must be able to control their services, as well as have access to tools that precisely characterise all of their interactions, in order to develop an accurate mental map of their virtual environment. In this view, trust encompasses more than just techniques that help objects interact with less ambiguity, yet these mechanisms are important for objects to select the best partner for their requirements [1]. Such IoT mechanisms must also be capable of determining trust in a dynamic and collaborative context, as well as comprehending the meaning of trust that must be delivered during the interaction.

Integrity is a concern not only for IoT, but for every system that deals with hardware, software, or data. The integrity concept ensures that unauthorised hardware and software modifications are prevented, that unauthorised data modifications are not conducted by authorised or unauthorised personnel or processes, and that data are consistent both internally and externally [52,77,97]. This description can aid in the identification of numerous difficulties that integrity and trust systems must address. To deal with the unique characteristics of IoT devices, new distributed and lightweight authentication and integrity frameworks and techniques must be investigated.

Trust also indicates that users receive information that they believe to be true and of a certain quality and timeliness. The received information can be trustworthy (usable immediately), trustworthy with alteration (usable after alteration), or untrustworthy (worthless) [49]. In the absence of trust, the user needs to consider whether it might be beneficial to abstain from using certain services of IoT. Thus, trust is one of the fundamental considerations for developing IoT laws and regulations that enable user rights.

IoT technology and applications can only be implemented on a broad scale if security is assured. The varying security requirements of the many domains of application is one challenge. Data protection is critical in the healthcare sector, for example, and the authenticity and security of data are critical in smart city applications. The protection of privacy is another important factor in the proliferation of IoT. Private data revealing movements, habits, or interactions with other persons must be adequately protected to address this issue [98]. In 2003, the revelation by clothing store Benetton that all items would be tagged with RFID-T transponders sparked widespread public outrage. As a result, the company was subjected to a widespread boycott [64,72]. While data collecting on the internet necessitates user's active participation, IoT apps include those who do not knowingly use these services.

The dropping cost of data storage is another factor that raises data security issues. This means that data collected once can theoretically be linked to data collected considerably later and stored for as long as required. One option would be to limit the information's use to a set time frame, after which it would be deleted. In practice, however, this is difficult to prove [56]. Because IoT is so closely linked to humans, many trust issues have arisen as a result of the rapid expansion in the use of IoT applications. When practically everything is connected to the global internet and things, and these vulnerabilities become more apparent, continued exposure will disclose more security and privacy issues, such as data integrity sensed and exchanged by things, secrecy, and authenticity [12,78]. Furthermore, in order to promote user privacy, reliable data integrity, and information security, the trust issue is crucial in IoT. As a result, it can assist people in adopting this technology. Despite this, there is not a complete study on trust in IoT systems in the literature.

3. Methodology

The aim of this study was achieved by employing a systematic literature review approach followed by a bibliometrics analysis. A systematic literature review (SLR) is a rigorous and systematic method of reviewing the existing literature in a specific research field. Such reviews are often used to identify patterns, trends, gaps, and strengths and weaknesses in existing research. The review provides valuable insights into the current state of the field and helps guide future research and development efforts in IoT. The review is based on planning, conducting, analysis, and reporting to identify and critically synthesise the published IoT work, following the works of [99,100] and answering the following research questions:

(1) What are the key applications of IoT in healthcare and banking industries that have been widely accepted by society?
(2) What are the social and organisational drivers of the continuous implementation of IoT in these sectors?
(3) What are the social and organisational challenges faced by these sectors when implementing IoT?

These research questions will not only enable multiple stakeholders such as researchers, academics, and practitioners to understand the use of IoT in healthcare and banking sectors but will also critically evaluate and highlight the importance of considering the social implications of IoT and taking appropriate steps to mitigate any negative effects. The development and use of IoT must be guided by a responsible and ethical approach that prioritises privacy, security, and well-being. The healthcare and banking sectors are some of the most sensitive industries in which IoT devices are widely implemented. As the personal information of customers is involved in both sectors, it becomes very case-sensitive when implementing and using IoT devices to a great extent.

3.1. Search and Selection

A structured literature search was conducted across four major databases—Web of Science, IEEExplore, Emerald Insight, and ScienceDirect—focusing on reputable, peer-reviewed English-language publications from 2012 onward. In this review, we only looked at research that specifically addressed IoT implications in both these sectors, focusing on social and organisational implications in broad terms to provide a combined effect of knowledge. As a result, we considered articles released after 2012 as this period saw a hike in publications related to the relevant domain. The search strategy combined constant keywords (e.g., "Internet of Things (IoT)", "Healthcare", "Banking", "Social", "Organisational") with a set of relative terms (e.g., "Adoption", "Trust", "Consumer satisfaction", etc.) using logical Boolean operators.

Given the topic is still new and active, we repeated the procedure of seeking, reviewing, and selecting relevant publications several times (Figure 3). A four-level screening was applied to define the eligibility of the articles and their inclusion in the review looking into whether the article deals with IoT in healthcare and/or banking, relates technology with society, and discusses drivers and challenges. The inclusion criteria (Table 3) ensured that studies addressed IoT in healthcare and/or banking, linked technology with societal themes, and discussed associated challenges and drivers. Finally, 110 studies were chosen out of 1387. Approximately 15% of the selected material came from conference proceedings and book chapters.

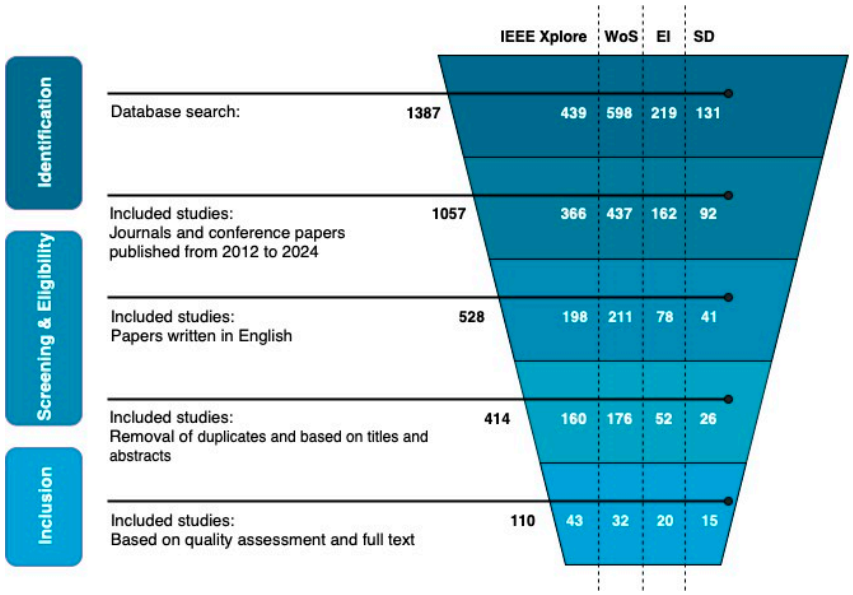

Figure 3. Process of article selection for the review.

Table 3. SLR inclusion and exclusion criteria.

Criteria Type	Inclusion Criteria	Exclusion Criteria
Time Frame	Articles published from 2012 onwards	Articles published before 2012
Language	English	Non-English publications
Document Type	Peer-reviewed journal articles, review papers, book chapters, conference papers, and early access articles	White papers, industry magazines, blogs, non-peer-reviewed sources
Subject Focus	Studies discussing IoT in the context of healthcare and/or banking	Studies focusing on unrelated sectors

Table 3. *Cont.*

Criteria Type	Inclusion Criteria	Exclusion Criteria
Thematic Focus	Research addressing social and/or organisational impacts of IoT	Studies focused solely on technical, architectural, or engineering aspects
Search Keywords	Articles including combinations of constant keywords (e.g., IoT, Healthcare, Banking, Social, Organisational) with relevant terms (e.g., Adoption, Trust, Automation)	Articles lacking these keyword combinations
Relevance	Studies linking IoT to societal or organisational drivers, challenges, or user experience	Studies only address IoT deployment without social or organisational context

3.2. Thematic Analysis

To categorise and synthesise the findings from the selected 110 studies, a manual thematic analysis approach was employed. This involved a careful reading of each study's abstract and outcome to identify key topics, research focuses, and application areas within the IoT literature. Studies that shared similar research objectives, technological applications, or theoretical perspectives were grouped together into thematic categories. This process resulted in the identification of five main research themes: (1) IoT applications in healthcare and security, (2) smart systems and IoT integration, (3) government-driven IoT adoption, particularly in China, (4) IoT system modelling and quality frameworks, and (5) emerging IoT research initiatives from diverse global regions. This thematic categorisation, summarised in Table 4 and illustrated in Figure 4, allowed for a comprehensive understanding of the current state of research while also highlighting existing research gaps and future research opportunities within each thematic area. Table 5 presents the descriptive summary of the selected works.

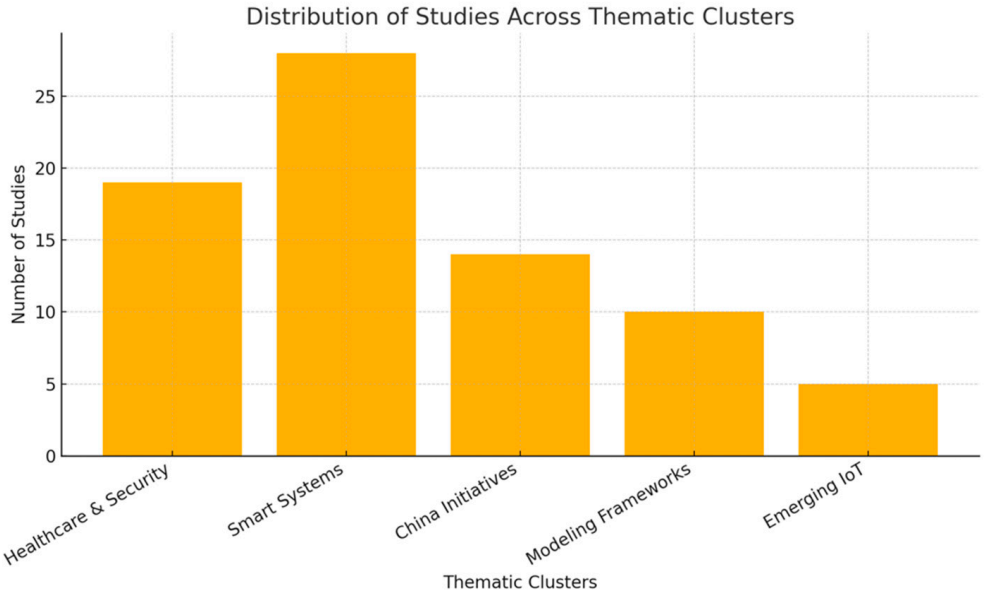

Figure 4. Distribution of the selected studies across thematic clusters.

Table 4. Summary of the thematic clusters, key contributions, and research gaps.

Cluster	Theme/Focus Area	Key Contributions	Research Gaps
Cluster 0	IoT applications in healthcare and security	- IoT for healthcare monitoring and diagnostics - Secure data sharing for patient privacy - Improved healthcare services through IoT	- Limited interoperability across platforms - Few real-world deployment studies - Ethical and regulatory concerns not fully addressed
Cluster 1	Smart systems and IoT integration	- Smart city and smart industry innovations - IoT integration with AI and machine learning - Intelligent automation in urban systems	- Underexplored rural and resource-constrained contexts - Lack of standardised integration frameworks - Sustainability issues underexplored
Cluster 2	IoT adoption in China and national initiatives	- Government-driven IoT projects - Policy-supported smart manufacturing - National infrastructure development for IoT	- Limited international or cross-cultural studies - Few critical evaluations of policy effectiveness - Lack of citizen engagement research
Cluster 3	IoT system modelling and quality frameworks	- Frameworks for IoT quality and reliability - System modelling and data-driven architectures - Real-time processing models	- Models are rarely empirically validated - Cybersecurity resilience underexplored - Industry 5.0 readiness not fully addressed
Cluster 4	Emerging IoT research and global initiatives	- Pilot IoT projects in diverse global regions - Applications in agriculture, education, and energy - Context-specific innovations	- Need for large-scale validation studies - Underrepresentation of developing regions - Lack of human-centric design exploration

Table 5. Descriptive summary of the selected studies.

Title	Authors	Year	Thematic Cluster
Privacy-Preserving and Secure Distributed Data Sharing Scheme for VANETs	Wang, L; Zhong, H; Cui, J; Zhang, J; Wei, L; Bolodurina, I; He, DB	2024	2
Taking Advantage of the Mistakes: Rethinking Clustered Federated Learning for IoT Anomaly Detection	Fan, JM; Wu, K; Tang, GM; Zhou, Y; Huang, SQ	2024	1
Digital-Twin-Inspired IoT-Assisted Intelligent Performance Analysis Framework for Electric Vehicles	Alsubai, S; Alqahtani, A; Alanazi, A; Bhatia, M	2024	1
Intelligent IoT and UAV-Assisted Architecture for Pipeline Monitoring in OGI	Karam, SN; Bilal, K; Shuja, J; Khan, LU; Bilal, M; Khan, MK	2024	1
Integrated Cyber-Physical Resiliency for Power Grids Under IoT-Enabled Dynamic Botnet Attacks	Zhao, YH; Chen, JT; Zhu, QY	2024	0
Galaxy: A Scalable BFT and Privacy-Preserving Pub/Sub IoT Data Sharing Framework Based on Blockchain	Zhang, YC; Wang, XT; He, XF; Zhang, N; Zheng, ZB; Xu, K	2024	2
Toward Secure and Reliable IoT Systems: A Comprehensive Review of Formal Methods Applications	Haddou-Oumouloud, I; Kriouile, A; Hamida, S; Ettalbi, A	2024	3
Internet of Things (IoT)-Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care	Balasundaram, A; Routray, S; Prabu, AV; Krishnan, P; Malla, PP; Maiti, M	2023	1
Recent Advances and Challenges in Internet of Things (IoT)-Based Smartphone Biosensors for COVID-19 and Zika Viruses Detection: A Review	Dehghani, A; Ghalamfarsa, F; Bidgoly, AJ; Mollarasouli, F	2023	1
Smart-IoT Business Process Management: A Case Study on Remote Digital Early Cardiac Arrhythmia Detection and Diagnosis	Gómez-Valiente, P; BenedÃ, JP; Lillo-Castellano, JM; Marina-Breysse, M	2023	1
Data for Societal Good: A Contextual Approach	Kaefer, F; Mora, G; Nath, R	2023	1
Dual-Task Network Embeddings for Influence Prediction in Social Internet of Things	Wang, F; She, JH; Wang, GJ; Ohyama, Y; Wu, M	2023	2
Capitalize Your Data: Optimal Selling Mechanisms for IoT Data Exchange	Li, QY; Li, Z; Zheng, ZZ; Wu, F; Tang, SJ; Zhang, Z; Chen, GH	2023	2

Table 5. *Cont.*

Title	Authors	Year	Thematic Cluster
IoT-Based Multi-Dimensional Chaos Mapping System for Secure and Fast Transmission of Visual Data in Smart Cities	Ahuja, B; Doriya, R; Salunke, S; Hashmi, MF; Gupta, A	2023	1
Three and a half decades of artificial intelligence in banking, financial services, and insurance: A systematic evolutionary review	Herrmann, H; Masawi, B	2022	1
Voice Activated IoT Devices for Healthcare: Design Challenges and Emerging Applications	Spachos, P; Gregori, S; Deen, MJ	2022	0
A Review of IoT-Enabled Mobile Healthcare: Technologies, Challenges, and Future Trends	Yang, YL; Wang, HC; Jiang, RZ; Guo, XN; Cheng, J; Chen, YY	2022	1
Investigating Industry 5.0 and Its Impact on the Banking Industry: Requirements, Approaches and Communications	Mehdiabadi, A; Shahabi, V; Shamsinejad, S; Amiri, M; Spulbar, C; Birau, R	2022	3
Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions	Aledhari, M; Razzak, R; Qolomany, B; Al-Fuqaha, A; Saeed, F	2022	0
Smart healthcare IoT applications based on fog computing: architecture, applications and challenges	Quy, VK; Hau, NV; Anh, DV; Ngoc, LA	2022	0
Impact of IoT on Manufacturing Industry 4.0: A New Triangular Systematic Review	Kalsoom, T; Ahmed, S; Rafi-ul-Shan, PM; Azmat, M; Akhtar, P; Pervez, Z; Imran, MA; Ur-Rehman, M	2021	3
Smart territories and IoT adoption by local authorities: A question of trust, efficiency, and relationship with the citizen–user–taxpayer.	Leroux, E; Pupion, PC	2022	4
Advanced data integration in banking, financial, and insurance software in the age of COVID-19	Maiti, M; Vukovic, D; Mukherjee, A; Paikarao, PD; Yadav, JK	2022	2
The role of the Internet of Things in Healthcare in supporting clinicians and patients: A narrative review	Lederman, R; Ben-Assuli, O; Vo, TH	2021	0
Internet of Things for Agricultural Applications: The State of the Art	Ojha, T; Misra, S; Raghuwanshi, NS	2021	1
Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT	Umair, M; Cheema, MA; Cheema, O; Li, H; Lu, H	2021	1
IoT Sensor Initiated Healthcare Data Security	Besher, KM; Subah, Z; Ali, MZ	2021	0
Scepticism and resistance to IoMT in healthcare: Application of behavioural reasoning theory with configurational perspective	Hajiheydari, N; Delgosha, MS; Olya, H	2021	0
Intelligent Edge Computing in Internet of Vehicles: A Joint Computation Offloading and Caching Solution	Ning, ZL; Zhang, KY; Wang, XJ; Guo, L; Hu, XP; Huang, J; Hu, B; Kwok, RYK	2021	2
The role of trust in intention to use the IoT in eHealth: Application of the modified UTAUT in a consumer context	Ben Arfi, W; Ben Nasr, I; Kondrateva, G; Hikkerova, L	2021	0
Privacy and the Internet of Things—An experiment in discrete choice	Goad, D; Collins, AT; Gal, U	2021	3
Mobile Edge Computing Enabled 5G Health Monitoring for Internet of Medical Things: A Decentralized Game Theoretic Approach	Ning, ZL; Dong, PR; Wang, XJ; Hu, XP; Guo, L; Hu, B; Guo, Y; Qiu, T; Kwok, RYK	2021	2
Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0	Kalsoom, T; Ramzan, N; Ahmed, S; Ur-Rehman, M	2020	1
A Self-Powered IoT Solution to Ease Predictive Maintenance in Substations	Kadechkar, A; Riba, JR; Moreno-Eguilaz, M; Perez, J	2020	1
Continuous Subsurface Tomography Over Cellular Internet of Things (IoT)	Jamali-Rad, H; van Beveren, V; Campman, X; van den Brand, J; Hohl, D	2020	1
A Cooperative Quality-Aware Service Access System for Social Internet of Vehicles (vol 5, pg 2506, 2018)	Ning, ZL; Hu, XP; Chen, ZK; Zhou, MC; Hu, B; Cheng, J; Obaidat, MS	2020	2
Ubiquitous and Low Power Vehicles Speed Monitoring for Intelligent Transport Systems	Choy, JLC; Wu, J; Long, CN; Lin, YB	2020	2
Estimating the impact of the Internet of Things on productivity in Europe	Espinoza, H; Kling, G; McGroarty, F; O'Mahony, M; Ziouvelou, X	2020	0
Low-Cost Diaper Wetness Detection Using Hydrogel-Based RFID Tags	Sen, P; Kantareddy, SNR; Bhattacharyya, R; Sarma, SE; Siegel, JE	2020	1
A review of challenges and barriers implementing RFID technology in the Healthcare sector	Abugabah, A; Nizamuddin, N; Abuqabbeh, A	2020	3
A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact	Chamola, V; Hassija, V; Gupta, V; Guizani, M	2020	1
The Internet of Things and economic growth in a panel of countries	Edquist, H; Goodridge, P; Haskel, J	2021	0
Mobile crowd sensing—Taxonomy, applications, challenges, and solutions	Boubiche, DE; Imran, M; Maqsood, A; Shoaib, M	2019	1

Table 5. *Cont.*

Title	Authors	Year	Thematic Cluster
Impact of customers' digital banking adoption on hidden defection: A combined analytical–empirical approach	Son, Y; Kwon, HE; Tayi, GK; Oh, W	2020	0
Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review	Verma, A; Prakash, S; Srivastava, V; Kumar, A; Mukhopadhyay, SC	2019	1
Blockchain in IoT Systems: End-to-End Delay Evaluation	Alaslani, M; Nawab, F; Shihada, B	2019	1
Sensors and Systems for Wearable Environmental Monitoring Toward IoT-Enabled Applications: A Review	Al Mamun, MA; Yuce, MR	2019	1
A systemic perspective on socioeconomic transformation in the digital age	Strohmaier, R; Schuetz, M; Vannuccini, S	2019	1
Subordinate Resolution—An Empirical Analysis of European Union Subsidiary Banks	Conlon, T; Cotter, J	2019	2
The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products	Jalali, MS; Kaiser, JP; Siegel, M; Madnick, S	2019	1
Willingness to provide personal information: Perspective of privacy calculus in IoT services	Kim, D; Park, K; Park, Y; Ahn, JH	2019	0
The Effect of Security, Privacy, Familiarity, and Trust on User's Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception	Alraja, MN; Farooque, MMJ; Khashab, B	2019	0
Impact of digital trends using IoT on banking processes	Khanboubi, F; Boulmakoul, A; Tabaa, M	2019	3
Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations	Neshenko, N; Bou-Harb, E; Crichigno, J; Kaddoum, G; Ghani, N	2019	1
An IoT-Based Intelligent Wound Monitoring System	Sattar, H; Bajwa, IS; Ul Amin, R; Sarwar, N; Jamil, N; Malik, MGA; Mahmood, A; Shafi, U	2019	0
Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs	Xie, LX; Ding, Y; Yang, HY; Wang, XM	2019	2
A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols	Tomic, I; McCann, JA	2017	0
Review of IoT applications in agro-industrial and environmental fields	Talavera, JM; Tobón, LE; Gómez, JA; Culman, MA; Aranda, JM; Parra, DT; Quiroz, LA; Hoyos, A; Garreta, LE	2017	0
A Survey on Security and Privacy Issues in Internet-of-Things	Yang, YC; Wu, LF; Yin, GS; Li, LJ; Zhao, HB	2017	2
Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm	Atzori, L; Iera, A; Morabito, G	2017	3
Big data and Internet of Things (IoT) technologies in Omani banks: a case study	Saxena, S; Al-Tamimi, TASM	2017	0
Measuring the Socioeconomic and Environmental Effects of Energy Efficiency Investments for a More Sustainable Spanish Economy	Medina, A; Camara, A; Monrobel, JR	2016	3
BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network	Gope, P; Hwang, T	2016	0
Trust Management in Social Internet of Things: A Survey	Abdelghani, W; Zayani, CA; Amous, I; Sèdes, F	2016	4
Economic and Social Implications of the Internet of Things in Europe in Relation to Business	Maresová, P; Kacetl, J	2016	4
Implementing Smart Factory of Industrie 4.0: An Outlook	Wang, SY; Wan, JF; Li, D; Zhang, CH	2016	2
A systematic literature review of studies on business process modeling quality	Moreno-Montes de Oca, I; Snoeck, M; Reijers, HA; Rodríguez-Morffi, A	2015	3
Resource Management Mechanism for SLA Provisioning on Cloud Computing for IoT	Choi, Y; Lim, Y	2015	4
Middleware for Internet of Things: a study	Fersi, G	2015	4
Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare	Rahmani, AM; Thanigaivelan, NK; Gia, TN; Granados, J; Negash, B; Liljeberg, P; Tenhunen, H	2015	1
Insurance Telematics: Opportunities and Challenges with the Smartphone Solution	Handel, P; Skog, I; Wahlstrom, J; Bonawiede, F; Welch, R; Ohlsson, J; Ohlsson, M	2014	3

Table 5. *Cont.*

Title	Authors	Year	Thematic Cluster
A Survey on Internet of Things From Industrial Market Perspective	Perera, C; Liu, CH; Jayawardena, S; Chen, M	2014	0
A socio-economic analysis of Smart Infrastructure sensor technology	Morimoto, R	2013	1
Network Coding for Efficient Error Recovery in Wireless Sensor Networks for Medical Applications	Marinkovic, S; Popovici, E	2009	2
E-Banking: Issues and Challenges	Nami, MR	2009	1
Living in a world of smart everyday objects—Social, economic, and ethical implications	Bohn, J; Coroama, V; Langheinrich, M; Mattern, F; Rohs, M	2004	1

3.3. Bibliometrics Analysis

Bibliometrics analysis is a valuable tool to trace the intellectual structure of a specific field of research. It allows for conducting a more structured literature review, including information and detecting patterns. We conducted a bibliometrics analysis using VOSViewer v1.6.20 software. We have chosen this software for its flexibility and compatibility with the data file formats (such as .RIS or .txt). The initial research information system (RIS) citations file data were obtained from the Web of Science. Figure 5 shows the publication distribution from 2012 to 2024. It is clear that there has been a sharp increase in the number of publications since 2014, indicating an increased interest in the subject. However, a sudden increase in the number of publications on relevant topics can be seen from 2020 onwards, which can be justified by the dependence of healthcare and banking sectors on technology during the pandemic. Considering journals with at least five related articles, it was noted that *IEEE Access* (9.4%) and the *IEEE Internet of Things Journal* (8.49%) both published about 17.9% of the articles. This could be a sign of these two journals' willingness to publish in the field of disruptive and innovative technologies. It could also be because these two journals are highly ranked in terms of recent impact factors.

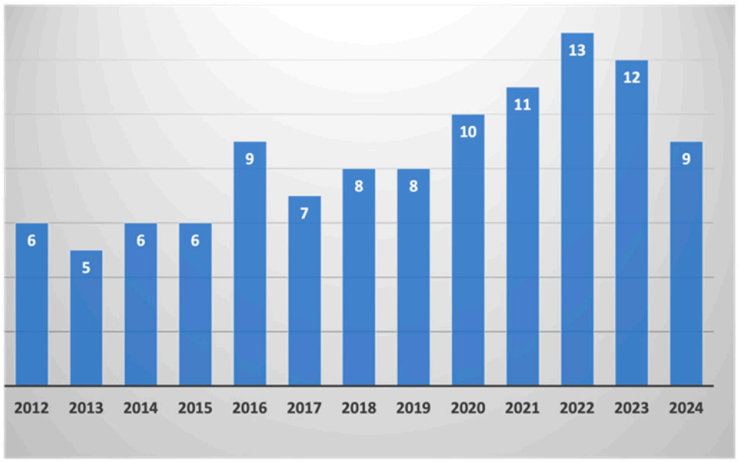

Figure 5. Year of publications included in the review.

1. *Division of Articles:* The papers were then divided into five groups based on the social elements of IoT perception, according to [101,102]. These groups were relation management, scalability, navigability, trust, and information processing (throughput and time). It was worth noting that a paper can fit into multiple categories. The majority of the papers, as seen in Figure 6, are associated with trust and information processing groups. A smaller number of researchers were interested in the social impact of IoT in relation to management. This can be explained by the fact that IoT technologies have been associated more with trust in terms of security and privacy of data, as well as the suitability of IoT to process huge amounts of data. It is anticipated

that navigability and scalability will be given a higher level of interest by academics given the rise of IoT devices in both healthcare and banking sectors.

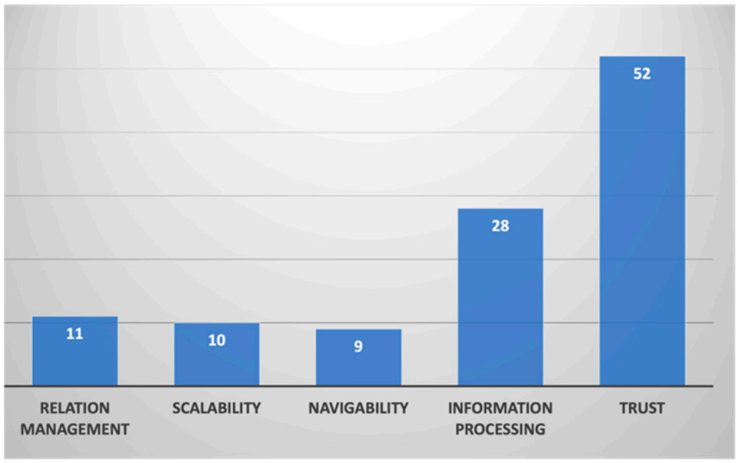

Figure 6. Distribution of articles based on social elements of IoT.

We also categorised the reviewed literature by contribution type (conceptual framework or review) and methodology (analytical, empirical, or case study) as illustrated in Figure 7. It was noted that a paper can belong to more than one category. The majority of authors presented conceptual frameworks or reviews for details in applying IoT-related concepts in healthcare and banking, as shown in Figure 6. For a new field, there are fewer analytical or empirical studies, which is understandable. However, we saw an increase in their number in 2016 and 2017. This shows that there is a need for academics to focus more on empirical studies when targeting social issues of IoT to gain an in-depth understanding of IoT's societal adoption.

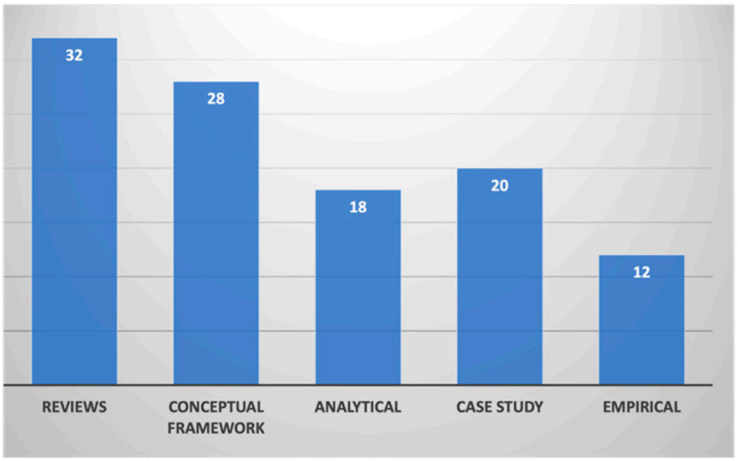

Figure 7. Types of publications included in the review.

2. *Network Visualisations of the Analysis:* Using VOSviewer, we created a network map of country co-authorship. As shown in Figure 8, clusters are established by the frequency of recurrence. The diameter of the circle represents the number of publications, while the thickness of the line shows the size of partnerships. Four clusters of 40 countries were discovered to contribute to the most comprehensive network of links by working on more than five publications. Furthermore, the USA, England, and Germany demonstrated the most extensive collaboration with other countries, indicating a high number of research and collaboration is being carried out in these countries on the related topic, followed by Italy, France, Brazil, and Canada. This also indicates that

IoT has been the focus of research by developed countries rather than developing or under-developed countries. A reason behind this can be that developed countries are the innovators and early adopters of IoT compared to developing countries, and these countries have seen the far-reaching impacts of IoT on society in recent years. As a result, it can be said that there is a need to focus on the adoption of IoT in developing countries as they are the ones that would enhance the current body of knowledge on the human-centric aspect of IoT adoption due to being new to technology awareness within these countries.

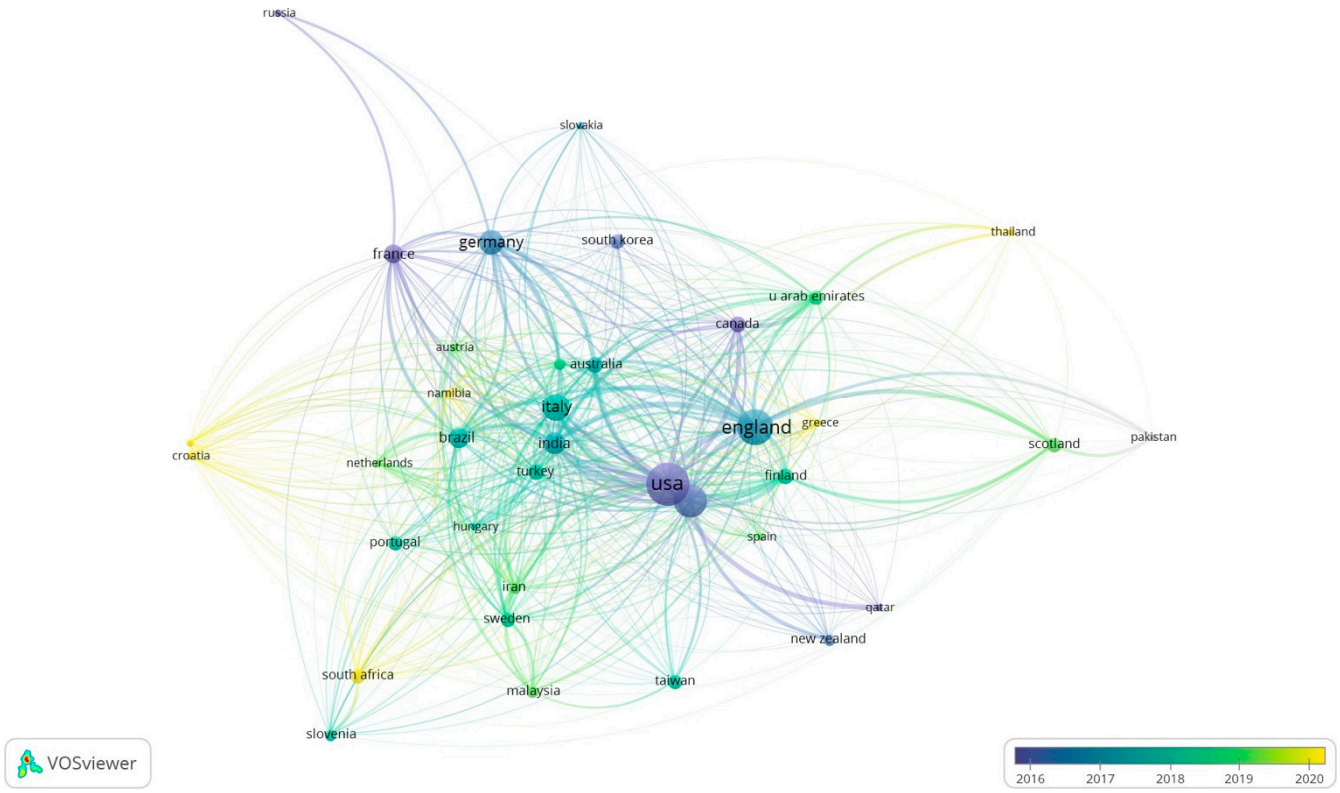

Figure 8. Network visualisation of country co-authorship.

A network visualisation of keyword co-occurrence was built by using VOSviewer (Figure 9). Based on the criteria that a keyword must appear in at least five publications to be considered, it was discovered that 100 out of 110 papers met the requirements. As a result of the analysis, 15 clusters were created, each with 600 links and a total link strength of 231. In addition, adoption was discovered to have the highest word frequency due to the strongest link strength with other words such as trust, patient, interaction, social connectedness, user, and person. Furthermore, current research has focused on terms like social internet, quality, and IoT systems. This suggests a rapid increase in the number of studies undertaken utilising the above-mentioned keywords. In addition, this also indicates a rapid increase in the use of these keywords in existing studies.

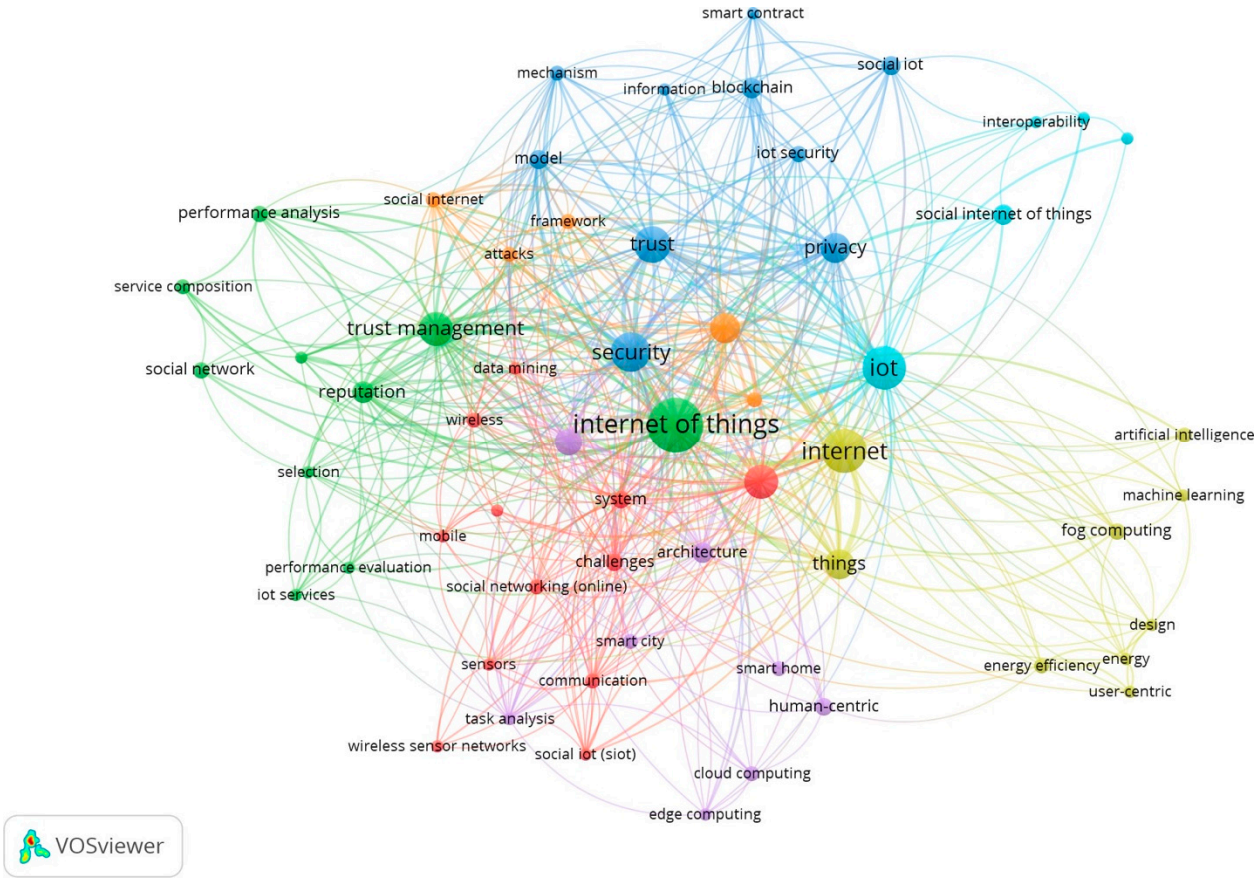

Figure 9. Network visualisation of keywords used for SLR.

4. Social and Organisational Impact of IoT

IoT will play a major role in next-generation healthcare systems due to its ability to automate patient care workflow. The healthcare sector is currently using IoT in two ways: in hospital and out of the hospital. In hospitals, IoT is used to manage hospital systems more effectively, such as developing wearable technologies that can help reduce costs and improve quality in the healthcare of patients. It also includes data-gathering sensors and RFID chips, which can help in providing advanced controls in hospitals and asset management and process optimisation in healthcare [103]. On the other hand, outside the hospital, autonomous systems make healthcare easy for both patients and doctors. For instance, when a patient's prescription is getting low, an automatic appointment with the physician can be set up just by a simple notification. Big data can help doctors and physicians to prescribe more effective medicines and cure complex diseases. Whether one is an elderly patient or a simple youth who wants to know about a medical condition, IoT is at the rescue. In this way, society is becoming more and more health conscious and healthier [104]. However, there are some challenges faced by society as well.

Based on the body of literature, it has been revealed that the behaviour of healthcare professionals in adopting and using IoT is not the same as other IoT users. This might be because of the distinctive characteristics of healthcare professionals regarding specialised training, autonomous practices, and professional work settings [103]. Studies have shown that some healthcare professionals are unwilling to use IoT systems for two main reasons: (1) fear of new applications and systems; and (2) fear of bringing changes in their core care practices [59,95,105]. This also highlights the issue some of these professionals face in terms of low computer literacy rates due to their established work routines and high professional autonomy. This reveals the need to provide special IT training to healthcare professionals to

successfully implement IoT in the healthcare sector. On the other hand, privacy issues of IoT devices acquire a new dimension in terms of social acceptance [106]. e-health uses electronic health records (EHRs), which contain unique patient identifiers (UPIs) [95]. This is to make sure that not only are EHRs accessible to healthcare professionals on an as-needed basis but also to guarantee that the right person receives the right intervention at the right time. Aside from the technical issues related to this architecture, there are underlying ethical and legal concerns on the issue of UPIs that need to be addressed [103,107]. Moreover, risks to patient data usage in some sensitive areas such as substance use or violence may pose certain challenges [79]. For instance, patients need to be informed about the rationale and benefits of data sharing with public health officials. Health institutions need to acquire consent from patients concerning data sharing [17,66]. In addition, some healthcare administrators may turn to specialised outsourcing to manage information and data management [59]. Although this action enables health institutions to provide cost-effective and cost–benefit services as global players are capable of providing relevant technologies and services at lower costs, this raises privacy concerns to a new level.

Another issue lies in the assumption that e-health instrumentation will provide patient data without constant technical supervision, as this would result in an intolerable intervention in the lives of patients [103,107]. In addition, the role of e-health workers increases as they now not only need to clinically check patients but also have to explain the uses and functions of IoT devices to them [108]. Therefore, e-health requires patients to understand the functionally important aspects of the technology with which they are involved because their actions may interfere with or alter the functioning of relevant protocols and devices [9]. Nonetheless, none of these issues detract from the promise of cost-effectiveness and efficiency that is presented by e-health. However, the above-mentioned issues need to be addressed before the technology is applied.

IoT facilitates automating cashless payments. Therefore, the banking sector is one of the most dependent sectors on IoT these days [109]. Not only does IoT help in providing better banking services to customers, but it also facilitates the production of big data about customers' behaviours, which in turn helps the bank to design and launch more customer-specific schemes [10]. Furthermore, it provides useful information to the banks such as how many ATM kiosks should be placed in a locality and where more cash will be needed by analysing the data about cash flows. These days, banks are using IoT so much that a new term has been coined, i.e., "Bank of Things" [41]. The societal factors about such developments are, however, more positive than negative [110]. It helps enhance the business activity in a region by creating employment opportunities and in this way improving the cycle of growth.

There are certain conflicts that may arise between society and banking organisations. The banks need to provide the best services related to online banking. On-time services and customer satisfaction play an important role in defining the service quality and in turn the image of the banks [89]. In addition, privacy and security of data are important aspects that banks have to focus on. Having huge personal information and bank account details of their customers, without having a viable security system in place is dangerous to all parties [41]. Another factor that defines the success of e-banking is trust, especially when a customer carries out a financial transaction that requires full confidence in the medium being used, the site being used, the connection, etc. [111]. This may give rise to several questions in the minds of customers, such as was the transaction successfully processed? Is the password and ID secure? Therefore, trust plays an important role and defines the willingness of customers to engage in transactions with web merchants [84]. In addition, despite the benefits of online banking, some people do not participate in it at all. This is mainly because people are used to the traditional form of banking and it may take time

to break these habits. Therefore, awareness among customers about the benefits and ease of use of e-banking plays an important in defining the success of the banks [84]. All these factors pose societal challenges that need to be addressed to successfully implement and use e-banking.

4.1. The 5Cs of IoT

For many industries, IoT opens the door to intriguing new applications and prospects. However, it also carries with it tremendous obstacles that necessitate new ways of thinking in order to achieve mission-critical objectives. After a comprehensive literature review, we determined 5Cs of technological obstacles (5Cs of IoT as shown in Figure 10), which organisations must overcome to deliver successful IoT in both the healthcare and banking sectors. A strong foundation for implementation and deployment across the ecosystem will be built by having a comprehensive grasp of these problems and knowing what the major design and test concerns are. Throughout the product lifecycle, the correct design, validation, compliance testing, manufacturing, and security tools will help to ensure that IoT delivers on its promises.

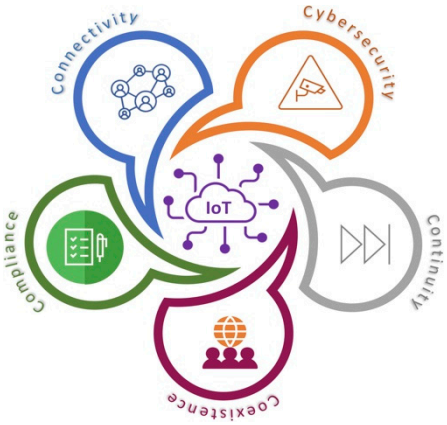

Figure 10. The 5Cs of the Internet of Things.

1. *Connectivity*: Because wireless communication is highly complex and dense device deployments further complicate operations, enabling a seamless flow of information to and from a device, infrastructure, cloud, and applications is a top IoT problem [84]. Even in the harshest settings, mission-critical IoT devices are expected to perform consistently and without failure. In healthcare, this is especially critical; for instance, remote patient monitoring systems rely on real-time connectivity to transmit vital signs to healthcare professionals. A dropped connection could result in missed alerts or delayed responses to emergencies. Fast-changing wireless standards add to the complication, and engineers are always challenged to stay up with the latest technology while ensuring that devices function together seamlessly across the ecosystem. Responding to connection difficulties necessitates the creation of extremely flexible and adjustable design and testing solutions that can be upgraded to meet future needs [112]. Flexibility is required to test devices with a variety of radio formats, to evaluate device performance in real-world scenarios, and to facilitate over-the-air (OTA) signal testing without the use of a chipset-specific driver. To reuse code and minimise measurement correlation difficulties across the many phases of development, the solution should be simple, economical, and able to be used in both R&D and manufacturing [6,112]. In banking, IoT devices like smart ATMs or biometric-enabled kiosks depend on stable connections for customer verification and transactions. In low-connectivity regions, service disruption can compromise user trust and opera-

tional efficiency. Solutions must be adaptable, allowing flexible testing and support for multiple radio formats and over-the-air protocols.

2. *Continuity*: One of the most essential aspects of IoT devices is ensuring and prolonging battery life. In consumer IoT devices, a long battery life is a big competitive advantage. The industry standard for industrial IoT devices is a battery life of five to ten years. In healthcare, device life can represent the difference between life and death for medical devices like pacemakers. Of course, a dead battery is not an option.

Integrated circuit (IC) designers must create ICs with deep sleep modes that consume very little current and reduce clock speed and instruction sets, as well as implement low battery voltages, to meet IoT battery life requirements. Standards groups are defining new low-power consumption operating modes for wireless communications, such as NB-IoT, LTE-M, LoRa, and Sigfox, which enable restricted active operation time while consuming minimal power [112]. In banking, mobile IoT devices used for real-time fraud detection or cardless withdrawals also require reliable operation, particularly in high-traffic branches or ATMs. Designers who include sensing, processing, control, and communication components into a finished product must understand how the peripherals operate and consume power, as well as optimise the product's firmware and software to simplify operation and reduce consumption.

3. *Compliance*: Radio standards and global regulatory criteria must be followed by IoT devices. Radio standards conformance and carrier acceptance tests, as well as regulatory compliance tests such as RF, EMC, and SAR tests, are all part of compliance testing [93]. Medical IoT devices must adhere to standards such as HIPAA (USA) or MDR (EU), which govern data privacy and medical safety. For example, a smart wearable that tracks heart rate must not only be accurate but also secure and compliant with data storage regulations. Therefore, design engineers are regularly pressed to fulfil short product launch timelines and ensure a smooth worldwide market entry while adhering to the most up-to-date laws.

Manual compliance testing might take days or weeks to complete since it is difficult and time-consuming. To stick to a product release timetable, designers should consider investing in in-house pre-compliance test solutions that can be used at any step of the design process to catch problems early [93]. Choosing one that is based on the test lab compliance system can also help to maintain measurement consistency and limit the possibility of measurement errors. In banking, IoT-enabled customer tracking tools or smart card readers must meet data protection regulations like GDPR, ensuring no unauthorised data collection or leakage. In-house compliance testing tools and early-stage pre-compliance assessments are vital for avoiding regulatory delays.

4. *Coexistence:* With billions of devices, radio channel congestion is an issue that is only going to become worse. In hospitals, multiple IoT systems—such as infusion pumps, monitors, and portable diagnostics—may compete for the same spectrum, potentially causing harmful interference. A malfunction due to radio collisions could disrupt patient care. Similarly, in banks using location-based IoT tracking systems, interference between customer devices and internal networks may affect service delivery or analytics accuracy. Standards bodies have created test procedures to evaluate device functioning in the presence of other signals to alleviate wireless congestion [1]. Adaptive frequency hopping (AFH), for example, allows a Bluetooth device to eliminate channels with a lot of data collisions. Listen before speak (LBT) and cooperative collision avoidance (CCA) are two further collision avoidance approaches that improve transmission efficacy. However, the effectiveness in a mixed-signal environment is unknown [1,112], and collisions and data losses will occur if the radio

formats do not identify each other. A medical infusion pump that stops working owing to environmental interference, or an industrial sensor that loses its control signal, can have disastrous repercussions. Coexistence testing is also essential for determining how a device will perform in a congested, mixed-signal environment, as well as the risk of maintaining wireless performance in the presence of unwanted signals present in the same operational environment [1].

5. *Cybersecurity:* The majority of traditional cybersecurity defence products have a network and cloud focus. Traditional cybersecurity measures often overlook IoT endpoints, which makes devices like health monitors or banking apps prime targets for exploitation. For instance, a compromised IoT device in a hospital could leak patient data or serve as an entry point for ransomware attacks. Vulnerabilities in endpoints and OTA are routinely neglected. While well-established technologies such as Bluetooth and WLAN are widely utilised, little research has been conducted to address OTA vulnerabilities [112]. Because of the intricacy of these wireless protocols, there may be hidden flaws in device radio implementations that allow hackers to gain access to or take control of a device. According to IDC, endpoints are responsible for 70% of security breaches. These IoT devices should be protected with extra caution [1]. Endpoint devices should be evaluated using a regularly updated database of known threats/attacks to monitor device responsiveness and discover anomalies, and OTA vulnerabilities and potential points of entry into endpoint devices should be found. In banking, wearable payment devices or smart wallets face threats of spoofing or data theft if not properly secured. Real-time threat databases and anomaly detection are essential for identifying vulnerabilities, especially in OTA environments.

4.2. Key Themes in Social Impact of IoT

The comprehensive SLR showed that industry strategy, innovations, sustainability, and transition issues were found to be the key issues in IoT adoption in healthcare and banking because of the unique challenges and opportunities presented by these sectors. In the healthcare sector, the adoption of IoT devices and technologies can improve patient outcomes, reduce costs, and increase efficiency. However, the industry must navigate issues related to data privacy and security, regulatory compliance, and the interoperability of different systems. In addition, healthcare providers must develop clear strategies for integrating IoT technologies into their existing workflows and systems.

Similarly, the banking industry is undergoing significant transformation as a result of the adoption of IoT technologies. Banks are using IoT devices to monitor customer behaviour, prevent fraud, and automate processes. However, the industry must also address issues related to data security, privacy, and compliance. Banks must also develop clear strategies for integrating IoT technologies into their existing systems and processes.

In both industries, sustainability is a key concern. The increased use of IoT devices and technologies can lead to higher energy consumption, increased waste, and greater environmental impact. To address these issues, healthcare and banking providers must consider the environmental impact of their IoT strategies and develop sustainable solutions.

Finally, the transition to IoT technologies requires significant investments in infrastructure, training, and change management. This requires a clear understanding of the potential benefits and risks associated with IoT adoption, as well as a clear plan for managing the transition process. Effective industry strategies, innovative solutions, and a focus on sustainability are critical to the successful adoption of IoT technologies in healthcare and banking.

1. *Industry Strategy:* Industry strategy refers to a plan of action developed by a company or an industry to achieve its long-term goals and objectives. It involves identifying the

current state of the industry, analysing trends, and forecasting future developments. The goal of industry strategy is to create a roadmap for success, which involves defining the company's competitive position, identifying growth opportunities, and developing plans for achieving those goals.

Industry strategy typically involves a comprehensive analysis of the market, including customer needs, competitive forces, and technological trends. This analysis helps to identify opportunities for growth and competitive advantage. Based on this analysis, the company or industry can then develop a plan for investment, resource allocation, and execution.

Industry strategy can have a significant impact on IoT adoption in healthcare and banking. The following are some ways that it can influence adoption:

- **Investment:** The level of investment made by healthcare and banking industries in IoT technology can impact its adoption. If these industries invest heavily in IoT technology, it can encourage adoption and create a more robust IoT ecosystem in healthcare and banking.
- **Standards and Regulations:** The healthcare and banking industries are highly regulated, and any new technology, including IoT, must meet strict standards and regulations. Industry strategy can influence the creation of these standards and regulations, which can either support or hinder IoT adoption in these industries.
- **Collaboration:** Collaboration between industry players and technology providers is crucial to the successful adoption of IoT in healthcare and banking. Industry strategy can encourage or discourage collaboration, which can have a significant impact on IoT adoption.
- **Data Security:** Healthcare and banking deal with sensitive personal data, and the security of these data is critical. Industry strategy can influence the development of secure IoT solutions that meet the data security requirements of these industries.

2. *Innovation and Technology:* Innovation in IoT refers to the development and implementation of new and creative ideas, technologies, and applications that enhance and advance the functionality, efficiency, and effectiveness of IoT systems. IoT innovation involves leveraging the power of sensors, devices, and connectivity to enable new capabilities and opportunities that were previously impossible or difficult to achieve. This may include using IoT to collect and analyse vast amounts of data to improve decision-making, automating processes and systems to increase efficiency and productivity, and creating new products and services that deliver value to customers and businesses. Innovation in IoT can also involve the integration of emerging technologies such as artificial intelligence, machine learning, and Blockchain to enhance the capabilities and functionality of IoT systems. By pushing the boundaries of what is possible with IoT, innovation can drive significant advances in fields such as healthcare, agriculture, transportation, and more.

Innovation and technology play a crucial role in the adoption of IoT in healthcare and banking. The following are some ways that they impact IoT adoption:

- **Advanced IoT Devices:** As IoT technology advances, new and more advanced devices are being developed for healthcare and banking. These devices offer more advanced features and functionalities, making them more attractive to healthcare and banking organisations.
- **Real-time Monitoring:** IoT technology allows for real-time monitoring of patient or customer health status and financial transactions. This can help healthcare providers and banking institutions to provide better and more efficient services to their customers.

- **Automation:** Automation of routine tasks, such as data collection and analysis, can help healthcare and banking organisations save time and reduce costs. This is particularly important in the healthcare industry, where staff shortages are a common problem.
- **Predictive Analytics:** IoT technology can be used to collect and analyse vast amounts of data, which can be used to predict future trends and outcomes. This can help healthcare and banking organisations to make more informed decisions and provide better services to their customers.
- **Telemedicine:** IoT technology can be used to provide remote healthcare services, such as telemedicine, which can help to reduce the burden on healthcare facilities and improve access to healthcare for patients in remote areas.

3. *Sustainability:* Sustainability plays a crucial role in IoT because it is essential to ensure that IoT devices and systems are environmentally responsible and socially sustainable. Social and sustainability factors can also have a significant impact on IoT adoption in healthcare and banking. Here are some ways they can influence the adoption:

- **Patient and Customer Trust:** Social and sustainability factors can influence patient and customer trust in healthcare and banking organisations. If these organisations are seen to be socially responsible and committed to sustainability, it can help to build trust and encourage the adoption of IoT solutions.
- **Ethical Considerations:** The use of IoT technology in healthcare and banking raises ethical considerations around data privacy and security, as well as the potential for discrimination or bias. Healthcare and banking organisations must consider these ethical considerations when implementing IoT solutions.
- **Environmental impact:** Sustainability considerations can also impact IoT adoption in healthcare and banking. Organisations may prioritise IoT solutions that are energy-efficient and have a low environmental impact.
- **Corporate Social Responsibility:** Healthcare and banking organisations have a responsibility to contribute to the greater social good. Adopting IoT solutions that have a positive impact on society, such as those that improve healthcare outcomes or financial inclusion, can align with corporate social responsibility goals.
- **Regulatory Compliance:** Sustainability and social factors can also impact regulatory compliance. Organisations may be required to comply with sustainability regulations or social responsibility standards, which can influence their adoption of IoT solutions.

4. *Transition Issues:* Transition issues are important to address in IoT because they are critical to ensuring the seamless and secure transfer of data between devices, networks, and applications. IoT devices typically operate in heterogeneous environments with diverse protocols, standards, and security requirements. These differences can create challenges for interoperability and data exchange between devices. Transition issues can arise in various areas of IoT, including network connectivity, device compatibility, data formatting, and security protocols. For instance, transitioning between different network protocols, such as Wi-Fi, Bluetooth, and cellular, can result in data loss or latency, leading to unreliable communication and slow response times. Similarly, transitioning between different data formats can cause interoperability issues, preventing devices from understanding each other's data. Addressing transition issues requires a coordinated effort from IoT manufacturers, developers, and network operators to ensure that IoT devices are designed with standard protocols and interfaces, that communication protocols are well defined and interoperable, and that security protocols are robust and up-to-date.

Transition issues can have a significant impact on IoT adoption in healthcare and banking. The following are some ways that they can influence adoption:

- **Legacy Systems:** Healthcare and banking organisations may have legacy systems that are incompatible with IoT solutions, making it difficult to transition to new technologies. Upgrading or replacing these systems can be time-consuming and expensive, which can slow down adoption.
- **Integration:** IoT solutions need to be integrated with existing systems and workflows to be effective. Healthcare and banking organisations may face integration challenges when adopting IoT solutions, which can impact adoption.
- **Staff Training:** Healthcare and banking organisations need to train their staff to use IoT solutions effectively. This can be a challenge, as IoT technology can be complex and require new skills and knowledge.
- **Cost:** IoT solutions can be expensive to implement, and healthcare and banking organizations may face financial challenges when transitioning to new technologies. The cost of IoT devices, software, and infrastructure can be a barrier to adoption.
- **Security:** IoT technology poses security risks, and healthcare and banking organisations need to ensure that they have robust security measures in place to protect their data and systems. Transitioning to IoT solutions can be challenging from a security perspective.
- **Lack of Familiarity:** Customers may not be familiar with IoT technology, and they may need to be educated about how to use IoT devices and services effectively. Organisations need to provide clear and concise instructions and training to help customers navigate IoT solutions.
- **Access to Technology:** Not all customers may have access to the technology required to use IoT solutions. In the healthcare sector, this can be a particular issue for elderly patients or those in remote areas. In the banking sector, this can be a particular issue for customers who do not have access to the internet or mobile devices.

4.3. Benefits of IoT

In the healthcare industry, IoT will largely enable applications in two areas: the domestic environment and hospital facilities [113]. In terms of applications for the domestic environment, the following three design domains provide significant possibilities for improving efficiency and quality:

- Emergency assistance and activity detection;
- Health monitoring and chronic disease support;
- Assistance systems and health-promoting living environment design.

Home emergency call systems are the most well-known form of emergency assistance. Traditional home emergency call systems require the user to press a button before an emergency call is made. This active involvement may become obsolete as a result of the Internet of Things. If motion sensors are installed in the home, they may sound an alarm if a person has fallen or has not moved for an unusually extended period of time [107]. To improve home care and medical care, health monitoring and assistance for chronic diseases include automatic remote and self-monitoring [114]. Another purpose is to encourage self-sufficiency to support a self-sufficient lifestyle [104]. Ambient Assisted Living (AAL) is a topic that has received a lot of scholarly interest in assistive technology and the design of a healthy living environment. This refers to "concepts, goods, and services that integrate modern technologies with the social environments of individuals affected" [16]. The goal is to improve the quality of life of people who require long-term assistance, to provide them with the appropriate medical care at the appropriate time, and to avoid unnecessary costs. Data security and system compatibility are the primary issues here [107]. The purpose of

medical facility applications is to "improve quality by providing more detailed information to medical and nursing staff and relieving them of administrative responsibilities" [107,115]. Sensors monitor the health of persons in need of assistance, and the data are stored and analysed in the cloud. The results of the analysis will subsequently be reported to the appropriate individuals [115]. This allows for better treatment quality. Nursing personnel, on the other hand, are no longer required to collect and analyse data, resulting in greater efficiency and cost savings [17].

IoT is evolving into a strong tool for what we can refer to as the Bank of Things (BoT). Users interact with the bank more when they are surrounded by connected devices. IoT devices collect data about a bank's customers [4]. This is how a financial institution gets to know its customers and better understands what services or goods they want [116]. Individual credit risks can be determined using data from social media and information about purchase behaviour, for example. Because of improved identification verification, IoT devices protect banking assets. Clients pay for purchases utilising fingerprints, retinal scans, and FaceIDs in mobile apps. Nymi, the smart wristband, records users' heartbeats; all you have to do to access the device is touch it with the bracelet.

When it comes to banking, the Internet of Things offers numerous benefits. This provides debtors and credit cardholders with dependable, easy-to-use services. Banks may track how consumers use ATM kiosks in different areas and adjust the number of ATMs installed in specific locations based on usage volumes [89]. Banks can also leverage the Internet of Things to bring on-demand services closer to clients by deploying kiosks and improving user access to financial services. IoT delivers customer data that enable banks to better understand their clients' business needs and value chains, including retailers, suppliers, and distributors [111]. The data also allow banks to learn more about their consumers. Banks can give value-added services, customised banking services and products, and financial help to customers using consumer information obtained through IoT [89,111].

4.4. Challenges of IoT

The most serious worry and threat that IoT technology poses in general, and in the healthcare business in particular, is the protection of patient personal information. IoT devices gather and transmit data in real time to the cloud for data analytics by design [116,117]. The infrastructure for receiving and processing data should be created and designed for scalability so that real-time data from millions of devices may be collected, processed, and stored for analytical models to derive insights. The majority of IoT devices that receive data, however, lack data protocols and standards. Furthermore, there is a great deal of ambiguity surrounding data ownership restrictions and privacy concerns [102]. Patient data obtained through various linked devices or wearables is vulnerable and valuable to hackers, who can use stolen data or information for medical identity theft or extortion. A hacker or criminal can exploit a patient's information to generate a phoney identification or purchase resalable medications or medical equipment. Cybercriminals can also file false insurance claims in the name of the patient [116].

More than ever before, the rising cost of healthcare continues to dominate the sector. IoT has not proven to offset the rising expenses of medical care; in fact, it has become more expensive [113]. The world is fast altering to adapt to the digital revolution and connected environment that we live in today. Many firms have had to re-evaluate their business, delivery, and support strategies due to the complexity of deploying IoT technologies and solutions [19]. Even with the emergence of IoT, the cost of modern medical treatment remains out of reach for the average and low-income groups. Even in industrialised economies, the expense of quality healthcare is always a major concern. This problem

in the healthcare business has given rise to a growing "Medical Tourism" industry, in which individuals with serious medical conditions can receive equivalent treatments in developing countries for a fraction of the cost [19,95].

The social and organisational impacts of benefits and challenges of IoT detailed in Tables 6 and 7, are summarised and illustrated in Figure 11.

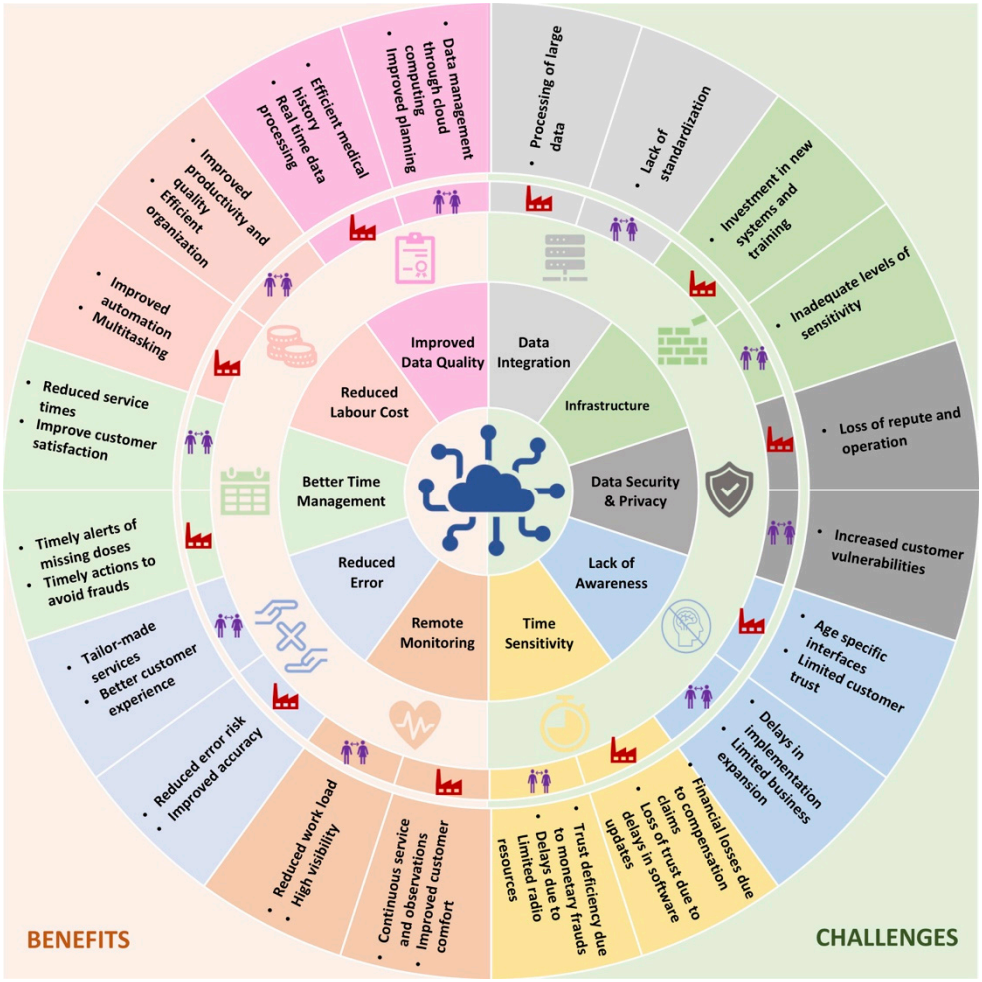

Figure 11. Social and organisational benefits and challenges of IoT adoption.

Table 6. Social and organisational impact of benefits of IoT.

Benefits	Social Impact	Organisational Impact
Improved data quality	• As more and more medical records become digitised, doctors and clinics can more efficiently track medical history and provide the treatment needed [117]. • As real-time information becomes visible to banks, they can identify and obtain useful insights into customer habits, hence reassuring healthcare and banking customers that their demands will be fulfilled in a timely manner.	• Issues related to e-healthcare such as data storage and management, security and privacy, and unified and universal access can be solved with the introduction of the cloud computing concept [118]. • Real-time and accurate insights into strategic threats and opportunities due to improved forecasting and trend analysis are experienced by organisations [119,120]. • Improved planning is employed with regard to management and maintenance.

Table 6. *Cont.*

Benefits	Social Impact	Organisational Impact
Reduced labour costs	• Healthcare could save GBP 90 billion in healthcare costs in the UK and add GBP 93 billion to the GDP by 2023 if IoT is adopted and encouraged. • As the load on healthcare services increases due to more demand for healthcare services rather than supply, there is a need to take multiple roles and perhaps multiple jobs [118]. IoT provides the opportunity to multitask effectively and efficiently.	• Reduction in costs due to insights into operational inefficiencies leads organisations to perform better in less costly environments. • Reduction in labour costs induces companies to hire more qualified workers. • Employee turnover reduces and there is an increase in employee productivity. • In healthcare with IoT, patient monitoring can be conducted in real time, drastically reducing the need for doctors to go out and make visits, thus reducing hospital stays and readmissions.
Better time management	• The main application of this technology is to remind the patient about their medication on time; for instance, if they forget one of their doses, it reminds them through timely alerts [118]. • In the banking sector, IoT enables banks to predict credit card fraud and debit transactions, which allows them to take appropriate action to prevent the problem in time.	• In healthcare, there is better time management in the case of emergency, where IoT analyses the distance and accesses patient profiles before they reach the hospital [117]. • Timely insights into customer demands and experience allow banks to enhance customer experience; for instance, customers know the exact time of their appointment by scheduling it using a smartphone app and can reach the counter at that time instead of waiting in the queue.
Reduced error	• IoT allows for accurate collection of data, automated workflows, and minimised waste, but most importantly it reduces the risk of error. • Accurate data enable correct diagnosis of diseases, which increases the interest of patients as well as doctors to improve diagnosis accuracy [118]. • Human error in patient data is reduced, which helps patients receive timely medications. • The development of wearables is a key factor in the widespread use of IoT in banking, with the potential of reducing error by biometric identification as opposed to vulnerable usernames and passwords.	• Healthcare and banking sectors can utilise accessible apps for tailored, timely delivery of personalised offers that are more likely to result in better customer experience and hence better relationships with organisations (both healthcare and banks).
Remote monitoring	• With real-time data, healthcare providers can continuously monitor patients. This means that they can spot any disease before it spreads and becomes serious. • M2M allows patients to be monitored in the comfort of their own homes. Sensors installed onto various medical apparatuses by the bedside of a patient can help data transfer to a medical specialist where it can be analysed for any abnormalities. • Bank customers can monitor their accounts with a single click on their smartphone apps and determine which transactions have taken place and where, thus reducing ATM fraud and thefts.	• Remote monitoring reduces home visits by healthcare providers, thus reducing workload and enhancing the productivity of employees. • With the remote monitoring ability, IoT devices allow banks to keep easy tabs in real time [119]. This helps them to maintain visibility into all the activities, even in unprecedented times.

There is no such thing as an "all-in-one" IoT solution. To realise the technology's full potential, a bank's IoT strategy must be devised and adapted to its main business objectives [89]. That said, such customisation and integration necessitate not only a significant commitment of time and money but also the selection of the correct IoT data management solution provider who is familiar with your organisation's hardware and software requirements [89]. The majority of banking institutions recognise that their customer data are critical to understanding their consumers, yet many lack the infrastructure to adequately digest and evaluate the data's impact on their business [111,116]. Many industry businesses lack the topic knowledge and skill set for collecting, storing, and repurposing data gathered

from IoT sensors when it comes to B2B data management. Furthermore, banks frequently face bottlenecks when it comes to cross-border enterprise-grade data transfers since they lack the necessary infrastructure to complete such activities securely and quickly.

One of the most significant issues that the financial sector faces is the capacity to securely share sensitive data with other network users while maintaining data integrity [121]. Removing this barrier to adoption entails training decision-makers on the many existing security standards so that organisations may reap the benefits of sharing information with other network users in a secure manner.

5. Lessons Learned

The social impact of IoT is a complex and multi-faceted issue that requires interdisciplinary research. Studies on the social impact of IoT need to consider the perspectives of multiple disciplines, including computer science, sociology, psychology, economics, and ethics. Social IoT has the potential to have a significant impact on society by improving the way people interact with each other and with technology. By conducting research in this area, researchers can contribute to the development of new technologies and applications that have real-world impact. It has been found that social IoT presents many challenges, such as privacy and security concerns, as well as opportunities, such as new ways to leverage social influence to promote positive behaviour change. Researchers can help to address these challenges and capitalise on these opportunities by conducting research in this area. The comprehensive SLR showed that one of the major challenges faced by IoT in healthcare and banking is the lack of interoperability between devices, systems, and platforms. A review of the literature showed that there is a need for standardisation in areas such as communication protocols, security, and data formats. In addition, the increasing number of connected devices in the IoT ecosystem raises serious security and privacy concerns. This literature review showed that there have been numerous studies and reports of security breaches and privacy violations in IoT systems, highlighting the need for stronger security measures and better privacy protection, which needs focus by both academics and practitioners. Moreover, the large amount of data generated by IoT devices presents a significant challenge for data storage, processing, and analysis. This literature review revealed that there have been numerous studies exploring different data management strategies and techniques for IoT systems but only some of the organisations have been successful in implementing them. Research has shown that regulation is needed to ensure the safe and responsible use of IoT. Regulations can help to ensure that IoT devices are secure, that personal data are protected, and that the rights of individuals are respected. Also, the widespread use of IoT devices has the potential to displace workers in many industries. Research has shown that the automation brought about by IoT devices may result in job loss and income inequality, which could have significant social and economic impacts. Although IoT use has countless benefits for its users, the widespread use of IoT devices has been linked to increased screen time, which can have negative effects on mental health and well-being. Research has shown that excessive use of screens can lead to depression, anxiety, and other mental health problems. This SLR highlighted the importance of considering the social implications of IoT and taking steps to mitigate any negative effects. The development and use of IoT must be guided by a responsible and ethical approach that prioritises privacy, security, and well-being.

Table 7. The social and organisational impacts of the challenges of IoT.

Challenges	Social Impact	Organisational Impact
Data integration and infrastructure	• Current healthcare and banking architecture does not reach the level of sensitivity required by IoT systems. • Most of the fraud occurs in both of these sectors due to the large size of data that need to be processed and compared with defined rules before triggering a personalised/financial decision [55,87]. Non-universality of these rules can make it very challenging.	• IoT adoption needs huge investments in new hardware and software systems along with personnel training to make the best use of it. • IoT adoption will enable healthcare and banking systems to have extensive information about the supply and production chain of their commercial customers [122]. These organisations will then have to analyse this wide range of information to meet the demands. • Healthcare and banking sectors dominated by IoT services require the ability to integrate huge volumes of data flow and to produce information in accordance with customers' needs and demands with enhanced infrastructure [79,123,124].
Data security and privacy	• By utilising IoT, a huge volume of data collected by healthcare and financial institutions from customers through different channels increases customer vulnerabilities. Data infringement and hacking may lead to massive damage to customers, resulting in disruption of the relationship between banks and their customers. • Customers face risks to their privacy in the form of phishing, virus attacks, unauthorised access, and fraudulent transactions [79,91,125]. For example, a phishing attack takes place when a customer opens an email linking it to a website, which prompts the customer to provide sensitive information regarding their bank accounts.	• Any data breach would lead to serious damages to healthcare institutions and banks in terms of reputation and financial damages [25,31,34,35]. • Although customers are advised to remain sensitive about these kinds of emails, the banks should adopt certain technologies to avoid such attacks in the future. • There is a potential risk of losing money as a result of an error in a transaction or a misuse of banking accounts [29,40].
Lack of awareness	• With older people being the recipients of several health services, WBANs need to be user-friendly and easy to use for them as most of this generation is not tech-savvy. Voice, gesture, and visual animation must be used to develop the user interface for disabled and elderly people [33,97,125]. • There are different groups of people with different interaction characteristics; therefore, the needs of these groups should be identified accordingly. For example, people with diabetes have different characteristics than patients with cognitive disorders. • Services such as e-banking are still not progressed in some countries due to inadequate trained human resources to adopt IoT. • Lack of information about services such as bank credit systems leads to limited business expansion of commercial banks, causing problems for individuals and SMEs in acquiring loans from the banks [124]. Many customers, therefore, remain unwilling to use this new channel and are reluctant to change from using the traditional services [76].	• Lack of awareness impacts both the healthcare and banking sectors in the context of facing difficulties in implementing new IoT solutions, with customers still preferring older methods of transactions. • User-friendly and natural interfaces must be provided to healthcare professionals to enable immediate response capabilities [70].
Time sensitivity	• A huge number of people are scared of using the internet for dealing with transactions in the sense of losing money in e-healthcare and online banking. • Delays in payments or navigation difficulties, such as finding suitable hyperlinks and services, may result in inconvenience and loss of time [81]. • A disorganised website and the slowness of downloading some web pages may upset customers.	• Not only customers but healthcare institutions and banks also face problems when customers look for compensation for any transaction errors that may have occurred [124]. • The length of time involved in waiting for websites, waiting to update an account, or learning new functionalities of the mobile applications may cause difficulties for customers, leading to a loss of trust and reputation of healthcare and banks [29,41,46].

6. Future Directions

Though IoT is promising to add great value to industry and the global economy, it poses several social issues on top of the technical challenges. It has been found that security problems and privacy fears are the prime concerns of society towards IoT implementation at a mass scale. In addition, ethical issues related to the implementation of IoT devices such as data security, the right to private life, rights to information sharing, etc., need to be taken into account by the stakeholders. Hence, the successful deployment of IoT makes the study of human response to the adoption of IoT services in our daily lives a necessity. Some of the future research directions are as follows:

6.1. Opportunistic IoT

As IoT devices evolve, the concept of Opportunistic IoT presents a human-centric model where smart devices form temporary, context-aware connections based on human social behaviour. Future research could explore how opportunistic interactions among individuals, such as shared locations or interests, can drive dynamic IoT networking and improve efficiency in data exchange. For instance, how these spontaneous links can be used to enhance community health monitoring or financial inclusion services is a question worth investigating. Simulation-based studies are particularly useful in this context, as they allow researchers to model complex human mobility patterns and social dynamics in a controlled environment, enabling large-scale testing of Opportunistic IoT behaviours without the ethical or logistical challenges of real-world trials. In addition, real-world field experiments using wearable devices could offer complementary insights into how Opportunistic IoT adapts to and reflects actual social structures.

6.2. Social IoT

Social IoT envisions a system where objects build social-like relationships, facilitating autonomous decision-making and collaborative task execution. However, the area of self-management within SIoT remains underexplored. Research should examine how devices in an SIoT ecosystem can autonomously manage trust, make decisions, and maintain secure interactions without continuous human intervention. This is especially relevant in healthcare environments where device collaboration is critical for patient care, or in banking where trust among connected devices is essential for secure transactions. Prototyping decentralised SIoT systems allows researchers to iteratively test and refine system behaviours in controlled conditions, while real-world deployments provide critical insights into interoperability, scalability, and user acceptance in complex, live environments. Together, these approaches can offer a comprehensive understanding of how SIoT functions under both experimental and practical conditions.

6.3. Social Accountability and Sustainability

As IoT becomes more embedded in personal and public life, its societal implications go far beyond technical functionality. While privacy remains a dominant concern, other issues—such as social equity, environmental sustainability, and ethical responsibility—are emerging as vital areas for investigation. Research could focus on how to embed social accountability into the IoT design process, ensuring that systems respect human values, avoid reinforcing inequalities, and promote responsible innovation. Examining regulatory frameworks enables a critical assessment of existing policies and helps identify gaps that may hinder ethical IoT adoption, while participatory design methods empower users and communities to directly shape the technologies that affect them. These approaches are particularly effective in capturing diverse perspectives and aligning technological solutions

with real societal needs, ultimately supporting the development of more inclusive and sustainable IoT ecosystems.

7. Conclusions

Sensors and Wi-Fi are changing the way people communicate with the surrounding world, bringing a new era of connectivity, termed the Internet of Things (IoT). This technology has the potential of providing virtually boundless opportunities to businesses and communities, with the enhanced connectivity and use of collected data. In this study, the applications and uses of IoT-based technologies widely accepted in the healthcare, manufacturing, and banking industries have been discussed in detail. By combining everyday objects with connected devices through IoT, it is possible to gather information, analyse it, and create an action to learn from processes. This research has shown that IoT technologies can help organisations automate and streamline their operations, leading to improved efficiency and cost savings. This can result in better profitability, higher productivity, and competitive advantage. Many other benefits of IoT on organisations have been indicated, such as a better understanding of their customer's needs and behaviours, leading to more personalised and effective customer experiences, resulting in increased customer satisfaction, loyalty, and retention. In addition, IoT technologies can enable organisations to develop new products and services, create new business models, and enter new markets, leading to innovation and growth opportunities. However, IoT devices can create security vulnerabilities, as they are often connected to networks and collect and transmit sensitive data. A security breach can lead to data loss, theft, and privacy violations. In addition, IoT technologies can add complexity to organisational systems, requiring specialised expertise to design, integrate, and manage. This can increase costs and create operational challenges. Moreover, IoT devices can replace human workers, leading to job displacement or requiring workers to develop new skills to adapt to the new technology.

Healthcare systems are one of the most important parts of our society and their crucial role has been demonstrated during the COVID-19 pandemic. Therefore, policymakers should be aware that proper decision-making and planning in this field are of utmost importance. The use of social IoT in healthcare systems has the potential to significantly improve patient outcomes, increase efficiency, and reduce costs. For example, remote patient monitoring, enhanced telemedicine, and improved communication between patients, healthcare providers, and caregivers can all result in better patient outcomes and improved quality of care. However, there are also privacy and security concerns that need to be addressed, as the collection and storage of sensitive personal health information raises significant concerns about data privacy and security.

In the banking industry, the use of social IoT has the potential to improve customer experience, increase efficiency, and reduce costs. For example, personalised services, real-time account updates, and improved risk management can all result in increased consumer satisfaction and improved financial outcomes. However, the use of IoT devices for financial transactions and data collection raises significant concerns about the security of financial information and the risk of fraud that need to be addressed.

It can be concluded that in both the healthcare and banking industries, it is important to consider the impact of social IoT on privacy and security and to take appropriate measures to mitigate these risks. This can include implementing robust security protocols, using encryption to protect sensitive information, and ensuring that data are stored securely. Additionally, it is important to consider the potential impact of social IoT on mental health and well-being and to take appropriate measures to minimise any negative consequences.

This study has several theoretical implications for researchers. In this regard, this research is a pioneering step that investigated the concept of IoT in the healthcare and bank-

ing sector focusing on the societal and organisational impacts. It can help researchers in this area to see the important attributes of the responsive IoT based on the adoption behaviour of people and apply these indicators to propose new frameworks that will further expand the domain. In other words, the main implication of this work for researchers is to present a list of criteria to study IoT adoption under societal and organisational considerations. Moreover, in today's hyper-competitive markets, especially with the dramatic growth of population and technologies, one of the major challenges for managers and practitioners is to appropriately manage their supply chains using IoT. In this context, this work can serve as a guiding note for the executives to improve the efficiency of their businesses by making them better understand the main goals of IoT, its dimensions, its applications in the healthcare and banking sectors, and society-led adoption issues. It can also help the administrators to integrate the indicators of social IoT and technologies, making them better acquainted with the concept of social IoT.

While this study provides valuable insights into IoT adoption within healthcare and banking, it does not account for other significant sectors such as manufacturing, agriculture, or transportation. This limits the generalisability of the findings to the broader IoT landscape. In addition, although this study references global literature, its case examples and contextual analysis are primarily drawn from the UK. This geographic focus may not reflect the social or organisational realities of IoT adoption in developing countries or regions with less digital infrastructure.

IoT is greatly influencing every aspect of human society. It is a known fact that IoT is the next technological marvel and it is rightly so. As an emerging service, this technology has many challenges in its full adoption by various communities and businesses. It has more pros than cons; however, the big data received by these connected devices, which are roughly more than 30 billion at the moment, can become dangerous if not utilised properly and sensibly due to privacy and security issues. This paper can help policymakers determine the most important factors of social IoT in healthcare and banking systems and establish policies to improve users' perception, acceptance, and experience of this promising technology, which can significantly contribute to its universal progress for the betterment of society.

Author Contributions: Conceptualization, T.K. and M.U.R.; methodology, T.K., N.R and S.A.; software, N.R.; validation, T.K. and S.A.; formal analysis, T.K.; investigation, T.K; resources, M.U.R. and G.A.S.; data curation, T.K. and N.A.; writing—original draft preparation, T.K.; writing—review and editing, G.A.S. and N.A.; visualization, T.K and M.U.R.; supervision, N.R. and S.A.; project administration, N.R. and S.A.; funding acquisition, N.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alam, M.; Shakil, K.A.; Khan, S. *Internet of Things (IoT): Concepts and Applications*; Springer: Berlin/Heidelberg, Germany, 2020.
2. Ojha, T.; Misra, S.; Raghuwanshi, N.S. Internet of things for agricultural applications: The state of the art. *IEEE Internet Things J.* **2021**, *8*, 10973–10997. [CrossRef]
3. Future Market Insights. The Enterprise IoT Market. 2023. Available online: https://www.globaltrademag.com/the-enterprise-iot-market-has-been-anticipated-to-rise-at-a-cagr-of-13-from-2023-to-2033-surpassing-us-2021-19-billion-by-2033/ (accessed on 16 April 2025).
4. Imran, M.A.; Hussain, S.; Abbasi, Q.H. Wireless Automation as an Enabler for the Next Industrial Revolution. Wiley-IEEE Press: Chichester, UK, 2019.
5. Zhang, Y.; Wang, X.; He, X.; Zhang, N.; Zheng, Z.; Xu, K. Galaxy: A scalable bft and privacy-preserving pub/sub iot data sharing framework based on blockchain. *IEEE Internet Things J.* **2024**, *11*, 5222–5236. [CrossRef]

6. Kalsoom, T.; Ahmed, S.; Shan, P.M.R.U.; Azmat, M.; Akhtar, P.; Pervez, Z.; Imran, M.A.; Ur-Rehman, M. Impact of iot on manufacturing industry 4.0: A new triangular systematic review. *Sustainability* **2021**, *13*, 12506. [CrossRef]
7. Ning, Z.; Zhang, K.; Wang, X.; Guo, L.; Hu, X.; Huang, J.; Hu, B.; Kwok, R.Y.K. Intelligent edge computing in internet of vehicles: A joint computation offloading and caching solution. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 2212–2225. [CrossRef]
8. Ning, Z.; Hu, X.; Chen, Z.; Zhou, M.; Hu, B.; Cheng, J.; Obaidat, M.S. A cooperative quality-aware service access system for social internet of vehicles. *IEEE Internet Things J.* **2018**, *5*, 2506–2517. [CrossRef]
9. Ning, Z.; Dong, P.; Wang, X.; Hu, X.; Guo, L.; Hu, B.; Guo, Y.; Qiu, T.; Kwok, R.Y.K. Mobile edge computing enabled 5g health monitoring for internet of medical things: A decentralized game theoretic approach. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 463–478. [CrossRef]
10. Kaefer, F.; Mora, G.; Nath, R. Data for societal good: A contextual approach. *IEEE Technol. Soc. Mag.* **2023**, *42*, 108–116. [CrossRef]
11. Butun, I. *Industrial IoT: Challenges, Design Principles, Applications, and Security*; Springer: Berlin/Heidelberg, Germany, 2020.
12. Sodagari, S. Trends for mobile iot crowdsourcing privacy and security in the big data era. *IEEE Trans. Technol. Soc.* **2022**, *3*, 199–225. [CrossRef]
13. Bohn, J.; Coroama, V.; Langheinrich, M.; Mattern, F.; Rohs, M. Social economic and ethical implications of ambient intelligence and ubiquitous computing. In *Ambient Intelligence*; Weber, W., Rabaey, J., Aarts, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2005.
14. Corte-Real, N.; Ruivo, P.; Oliveira, T. Leveraging internet of things and big data analytics initiatives in european and american firms: Is data quality a way to extract business value? *Inf. Manag.* **2020**, *57*, 103141. [CrossRef]
15. Ahuja, B.; Doriya, R.; Salunke, S.; Hashmi, M.F.; Gupta, A. Iot-based multi-dimensional chaos mapping system for secure and fast transmission of visual data in smart cities. *IEEE Access* **2023**, *11*, 104930–104945. [CrossRef]
16. Choy, J.L.C.; Wu, J.; Long, C.; Lin, Y.-B. Ubiquitous and low power vehicles speed monitoring for intelligent transport systems. *IEEE Sens. J.* **2020**, *20*, 5656–5665. [CrossRef]
17. Goad, D.; Collins, A.T.; Gal, U. Privacy and the internet of things—An experiment in discrete choice. *Inf. Manag.* **2021**, *58*, 103292. [CrossRef]
18. Verma, A.; Prakash, S.; Srivastava, V.; Kumar, A.; Mukhopadhyay, S.C. Sensing, controlling, and IoT infrastructure in smart building: A review. *IEEE Sens. J.* **2019**, *19*, 9036–9046. [CrossRef]
19. Mamun, M.A.A.; Yuce, M.R. Sensors and systems for wearable environmental monitoring toward IoT-enabled ap-plications: A review. *IEEE Sens. J.* **2019**, *19*, 7771–7788. [CrossRef]
20. Boubiche, D.E.; Imran, M.; Maqsood, A.; Shoaib, M. Mobile crowd sensing-taxonomy, applications, challenges and solutions. *Comput. Hum. Behav.* **2019**, *101*, 352–370. [CrossRef]
21. Imran, M.A.; Sambo, Y.A.; Abbasi, Q.H. *Enabling 5G Communication Systems to Support Vertical Industries*; John Wiley & Sons Ltd.: West Sussex, UK, 2019.
22. Vermesan, O.; Friess, P. *Internet of Things Applications—From Research and Innovation to Market Deployment*; River Publishers: Aalborg, Denmark, 2014.
23. Crump, J.; Brown, I. The societal impact of internet of things. *Chart. Inst. IT* **2013**, *8*, 39–56.
24. Talavera, J.M.; Tobon, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.; Garreta, L.E. Review of IoT applications in agro-industrial and environmental fields. *Comput. Electron. Agric.* **2017**, *142*, 283–297. [CrossRef]
25. Rose, K.; Eldridge, S.; Chapin, L. The internet of things: An overview. *Internet Soc.* **2015**, *10*, 5–56.
26. Edquist, H.; Goodridge, P.; Haskel, J. The internet of things and economic growth in a panel of countries. *Econ. Innov. New Technol.* **2021**, *30*, 262–283. [CrossRef]
27. Strohmaier, R.; Schuetz, M.; Vannuccini, S. A systemic perspective on socioeconomic transformation in the digital age. *J. Ind. Bus. Econ.* **2019**, *46*, 361–378. [CrossRef]
28. Espinoza, H.; Kling, G.; McGroarty, F.; O'Mahony, M.; Ziouvelou, X. Estimating the impact of the internet of things on productivity in europe. *Heliyon* **2020**, *6*, e03935. [CrossRef] [PubMed]
29. Philip, B.V.; Alpcan, T.; Jin, J.; Palaniswami, M. Distributed real-time iot for autonomous vehicles. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1131–1140. [CrossRef]
30. Medina, A.; Camara, A.; Monrobel, J. Measuring the socio-economic and environmental effects of energy efficiency in-vestments for a more sustainable spanish economy. *Sustainability* **2016**, *8*, 1039. [CrossRef]
31. Wellman, B. Computer networks as social networks. *Science* **2001**, *293*, 2031–2034. [CrossRef]
32. PwC. Study to Examine the Socio-Economic Impact of Copernicus in the EU. European Commission, Tech. Rep. 2016. Available online: https://www.copernicus.eu/sites/default/files/2018-10/Copernicus_Report_Downstream_Sector_October_2016_0.pdf (accessed on 16 March 2025).
33. Balasundaram, A.; Routray, S.; Prabu, A.V.; Krishnan, P.; Malla, P.P.; Maiti, M. Internet of things (iot)-based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care. *IEEE Internet Things J.* **2023**, *10*, 18563–18570. [CrossRef]

34. Morimoto, R. A socio-economic analysis of Smart Infrastructure sensor technology. *Transp. Res. Part C Emerg. Technol.* **2013**, *31*, 18–29. [CrossRef]
35. BSR. Socioeconomic Impacts of Wireless Technology. CTIA–The Wireless Association, Tech. Rep. 2012. Available online: https://www.bsr.org/en/reports/socioeconomic-impacts-of-wireless-technology (accessed on 10 January 2025).
36. Irene, C.L.; Wakenshaw, S. The internet of things: A review and research directions. *Int. J. Res. Mark.* **2017**, *34*, 3–21.
37. Kanti, T.; Giri, J.N.; Bhatia, H.; Pandit, J.; Gupta, A. *Technological and Managerial Strategies for Next Generation Transformation*; Bloomsbury: London, UK, 2017.
38. Alaslani, M.; Nawab, F.; Shihada, B. Blockchain in iot systems: End-to-end delay evaluation. *IEEE Internet Things J.* **2019**, *6*, 8332–8344. [CrossRef]
39. Li, S.; Xu, S.; Zhao, S. Internet of things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259. [CrossRef]
40. Wang, F.; She, J.; Wang, G.; Ohyama, Y.; Wu, M. Dual-task network embeddings for influence prediction in social internet of things. *IEEE Internet Things J.* **2023**, *10*, 6586–6597. [CrossRef]
41. Rega, F.G. *The Bank of the Future, the Future of Banking—An Empirical Analysis of European Banks*; SSRN: London, UK, 2017; pp. 1–18. [CrossRef]
42. Oca, D.; Snoeck, M.; Reijers, H.A.; Morffi, A.R. A systematic literature review of studies on business process modelling quality. *Inf. Softw. Technol.* **2015**, *58*, 187–205.
43. Volk, R.; Stengel, J.; Schultmann, F. Building information midelling for existing buildings—Literature review and future needs. *Autom. Constr.* **2014**, *38*, 109–127.
44. Rainham, D. A wireless sensor network for urban environmental health monitoring. *IOP Sci. Conf. Ser. Earth Environ. Sci.* **2016**, *34*, 012028.
45. Choi, Y.; Lim, Y. Resource management mechanism for sla provisioning on cloud computing for iot. In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 28–30 October 2015; pp. 500–502.
46. Perera, C.; Liu, C.H.; Jayawardena, S.; Chen, M. A survey on internet of things from industrial market perspective. *IEEE Access* **2014**, *2*, 1660–1679. [CrossRef]
47. Stankovic, J.A. Research directions for the internet of things. *IEEE Internet Things J.* **2014**, *1*, 3–9. [CrossRef]
48. Citak, A.L.; Silahtaroglu, G. The internet of financial things: Today and future perspectives. *J. Eur. Theor. Appl. Stud.* **2017**, *5*, 1–10.
49. Yifter, T.; Mengstenew, M.; Yoseph, S.; Moges, W. Modeling and simulation of queuing system to improve service quality at commercial bank of Ethiopia. *Cogent Eng.* **2023**, *10*. [CrossRef]
50. Kadge, S.; Hasan, C.; Zilani, A.Q.; Jain, Y. Asset management based on internet of things. *Int. J. Comput. Appl.* **2016**, *137*, 50–55. [CrossRef]
51. Saxena, S.; Al-Tamimi, A.T. Big data and internet of things technologies in omani banks: A case study. *Foresight* **2017**, *19*, 409–420. [CrossRef]
52. Jamali-Rad, H.; van Beveren, V.; Campman, X.; Brand, J.v.D.; Hohl, D. Continuous subsurface tomography over cellular internet of things (iot). *IEEE Sens. J.* **2020**, *20*, 10079–10091. [CrossRef]
53. Kadechkar, A.; Riba, J.-R.; Moreno-Eguilaz, M.; Perez, J. Smartconnector: A self-powered iot solution to ease predictive maintenance in substations. *IEEE Sens. J.* **2020**, *20*, 11632–11641. [CrossRef]
54. Sen, P.; Kantareddy, S.N.R.; Bhattacharyya, R.; Sarma, S.E.; Siegel, J.E. Low-cost diaper wetness detection using hydrogel-based rfid tags. *IEEE Sens. J.* **2020**, *20*, 3293–3302. [CrossRef]
55. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
56. Atzori, L.; Iera, A.; Morabito, G. Understanding the internet of things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad. Hoc. Netw.* **2017**, *56*, 122–140. [CrossRef]
57. Gope, P.; Hwang, T. Bsn-care: A secure iot-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2016**, *16*, 1368–1376. [CrossRef]
58. Alraja, M.N.; Farooque, M.M.J.; Khashab, B. The effect of security, privacy, familiarity, and trust on users? attitudes toward the use of the iot-based healthcare: The mediation role of risk perception. *IEEE Access* **2019**, *7*, 111341–111354. [CrossRef]
59. Balas, V.E.; Pal, S. *Healthcare Paradigms in the Internet of Things Ecosystem*; Academic Press: Cambridge, MA, USA, 2020.
60. Sattar, H.; Bajwa, I.S.; Amin, R.U.; Sarwar, N.; Jamil, N.; Malik, M.G.A.; Mahmood, A.; Shafi, U. An iot-based intelligent wound monitoring system. *IEEE Access* **2019**, *7*, 144500–144515. [CrossRef]
61. Dehghani, A.; Ghalamfarsa, F.; Bidgoly, A.J.; Mollarasouli, F. Recent advances and challenges in internet of things (iot)-based smartphone biosensors for COVID-19 and zika viruses detection: A review. *IEEE Sens. J.* **2023**, *23*, 24123–24134. [CrossRef]
62. Spachos, P.; Gregori, S.; Deen, M.J. Voice activated iot devices for healthcare: Design challenges and emerging applications. *IEEE Trans. Circuits Syst. II Express Briefs* **2022**, *69*, 3101–3107. [CrossRef]

63. Sedov, V. Socio-economic impact of cloud enabled internet of things: The total economic impact of iot for microsoft. *Forrester Study Total Econ. Impact* **2016**, *2*, 1–36.
64. Abugabah, A.; Nizamuddin, N.; Abuqabbeh, A. A review of challenges and barriers implementing RFID technology in the Healthcare sector. *Procedia Comput. Sci.* **2020**, *170*, 1003–1010. [CrossRef]
65. Tomic, I.; McCann, J.A. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet Things J.* **2017**, *4*, 1910–1923. [CrossRef]
66. Rao, P.M.; Pedada, S.; Jangirala, S.; Das, A.K.; Rodrigues, J.J.P.C. Role of iot in the ages of digital to smart cities: Security challenges and countermeasures. *IEEE Internet Things Mag.* **2024**, *7*, 56–64. [CrossRef]
67. Li, Q.; Li, Z.; Zheng, Z.; Wu, F.; Tang, S.; Zhang, Z.; Chen, G. Capitalize your data: Optimal selling mechanisms for iot data exchange. *IEEE Trans. Mob. Comput.* **2023**, *22*, 1988–2000. [CrossRef]
68. Saidu, C.; Usman, A.; Ogedebe, P. Internet of things:impact on economy. *Br. J. Math. Comput. Sci.* **2015**, *1*, BIMCS2015119.
69. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in internet-of-things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
70. Razzaque, M.A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for internet of things: A survey. *IEEE Internet Things J.* **2016**, *3*, 70–95. [CrossRef]
71. Tony, D. Morgan Stanley: 75 Billion Devices Will Be Connected to the Internet of Things by 2020. 2016. Available online: https://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10 (accessed on 11 February 2025).
72. Leroux, E.; Pupion, P.-C. Smart territories and iot adoption by local authorities: A question of trust, efficiency, and relationship with the citizen- user-taxpayer. *Technol. Forecast. Soc. Change* **2021**, *174*, 121195. [CrossRef]
73. Das, T.; Shukla, R.M.; Sengupta, S. What could possibly go wrong? identification of current challenges and prospective opportunities for anomaly detection in internet of things. *IEEE Netw.* **2023**, *37*, 194–200. [CrossRef]
74. Handel, P.; Skog, I.; Wahlstrom, J.; Bonawiede, F.; Welch, R.; Ohlsson, J.; Ohlsson, M. Insurance telematics: Opportunities and challenges with the smartphone solution. *IEEE Intell. Transp. Syst. Mag.* **2014**, *6*, 57–70. [CrossRef]
75. Little, A. Socio-economic Effects of Broadband Speed. Ericsson, Tech. Rep. 3/221 01-FGB 101 0003. 2013. Available online: http://nova.ilsole24ore.com/wordpress/wp-content/uploads/2014/02/Ericsson.pdf (accessed on 5 February 2025).
76. Rahmani, A.-M.; Thanigaivelan, N.K.; Gia, T.N.; Granados, J.; Negash, B.; Liljeberg, P.; Tenhunen, H. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; pp. 826–834.
77. Zhao, Y.; Chen, J.; Zhu, Q. Integrated Cyber-Physical Resiliency for Power Grids Under IoT-Enabled Dynamic Botnet Attacks. *IEEE Trans. Control. Syst. Technol.* **2024**, *32*, 1755–1769. [CrossRef]
78. Schoenherr, J.R. Adoption of surveillance technologies: Data openness, privacy, and cultural tightness. *IEEE Trans. Technol. Soc.* **2021**, *2*, 122–127. [CrossRef]
79. Kim, D.; Park, K.; Park, Y.; Ahn, J.-H. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Comput. Hum. Behav.* **2019**, *92*, 273–281. [CrossRef]
80. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
81. Karam, S.N.; Bilal, K.; Shuja, J.; Khan, L.U.; Bilal, M.; Khan, M.K. Intelligent IoT- and UAV-Assisted Architecture for Pipeline Monitoring in OGI. *It Prof.* **2024**, *26*, 46–54. [CrossRef]
82. Wang, L.; Zhong, H.; Cui, J.; Zhang, J.; Wei, L.; Bolodurina, I.; He, D. Privacy-Preserving and Secure Distributed Data Sharing Scheme for VANETs. *IEEE Trans. Mob. Comput.* **2024**, *23*, 13882–13897. [CrossRef]
83. Maresova, P.; Kacetl, J. Economic and social implications of the internet of things in europe in relation to business. In *Business Challenges in the Changing Economic Landscape*; Bilgin, M., Danis, H., Demir, E., Can, U., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 2, pp. 155–163.
84. Khanboubi, F.; Boulmakoul, A.; Tabaa, M. Impact of digital trends using IoT on banking processes. *Procedia Comput. Sci.* **2019**, *151*, 77–84. [CrossRef]
85. Surekha, N.; Sangeetha, R.; Aarthy, C.; Kavitha, R.; Anuradha, R. *Leveraging Blockchain Technology for Internet of Things Powered Banking Sector*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 181–207.
86. Maiti, M.; Vukovia, D.; Mukherjee, A.; Paikarao, P.D.; Yadav, J.K. Advanced data integration in banking, financial, and insurance software in the age of COVID-19. *Softw. Pract. Exp.* **2022**, *52*, 887–903. [CrossRef]
87. Boumlik, A.; Bahaj, M. Big data and iot: A prime opportunity for banking industry. In *Advanced Information Technology, Services and Systems*; Ezziyyani, M., Bahaj, M., Khoukhi, F., Eds.; Springer: Berlin/Heidelberg, Germany, 2017.
88. Son, Y.; Kwon, H.E.; Tayi, G.K.; Oh, W. Impact of customers' digital banking adoption on hidden defection: A combined analytical–empirical approach. *J. Oper. Manag.* **2020**, *66*, 418–440. [CrossRef]
89. Farooqui, A.; Rajani, P. E-banking issues and challenges. *IOSR J. Bus. Manag.* **2019**, *19*, 31–39.

90. Alsubai, S.; Alqahtani, A.; Alanazi, A.; Bhatia, M. Digital-Twin-Inspired IoT-Assisted Intelligent Performance Analysis Framework for Electric Vehicles. *IEEE Internet Things J.* **2024**, *11*, 18880–18887. [CrossRef]
91. Haddou-Oumouloud, I.; Kriouile, A.; Hamida, S.; Ettalbi, A. Toward Secure and Reliable IoT Systems: A Comprehensive Review of Formal Methods Applications. *IEEE Access* **2024**, *12*, 171853–171875. [CrossRef]
92. Fan, J.; Wu, K.; Tang, G.; Zhou, Y.; Huang, S. Taking Advantage of the Mistakes: Rethinking Clustered Federated Learning for IoT Anomaly Detection. *IEEE Trans. Parallel Distrib. Syst.* **2024**, *35*, 862–876. [CrossRef]
93. Minani, J.B.; Sabir, F.; Moha, N.; Guéhéneuc, Y.-G. A multimethod study of internet of things systems testing in industry. *IEEE Internet Things J.* **2024**, *11*, 1662–1684. [CrossRef]
94. Besher, K.M.; Subah, Z.; Ali, M.Z. Iot sensor initiated healthcare data security. *IEEE Sens. J.* **2021**, *21*, 11977–11982. [CrossRef]
95. Abdelghani, W.; Zayani, C.A.; Amous, I.; Sedes, F. Trust management in social internet of things: A survey. In Proceedings of the Conference on E-Business, E-Services and E-Society, Swansea, UK, 13–15 September 2016.
96. Chang, S.; Huang, A.; Chang, L.; Liao, J. Risk factors of enterprise internal control: Governance refers to internet of things environment. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS), Chiayi, Taiwan, 27 June–1 July 2016.
97. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in internet of things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
98. Tranfield, D.; Denyer, D.; Smart, P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br. J. Manag.* **2003**, *14*, 207–222. [CrossRef]
99. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
100. Hassan, Q.F. *Internet of Things A to Z: Technologies and Applications*; Wiley-IEEE Press: Chichester, UK, 2018.
101. Shenkoya, T. Social change: A comparative analysis of the impact of the iot in japan, germany and australia. *Internet Things* **2020**, *11*, 100250. [CrossRef]
102. Kluge, E.H.W. E-health and its challenges. *Health Manag.* **2017**, *5*. Available online: https://healthmanagement.org/c/it/IssueArticle/e-health-and-its-challenges (accessed on 16 April 2025).
103. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M. A comprehensive review of the COVID-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. *IEEE Access* **2020**, *8*, 90225–90265. [CrossRef]
104. Quy, V.K.; Hau, N.V.; Anh, D.V.; Ngoc, L.A. Smart healthcare iot applications based on fog computing: Architecture, applications and challenges. *Complex Intell. Syst.* **2022**, *8*, 3805–3815. [CrossRef] [PubMed]
105. Yang, Y.; Wang, H.; Jiang, R.; Guo, X.; Cheng, J.; Chen, Y. A review of iot-enabled mobile healthcare: Technologies, chal-lenges, and future trends. *IEEE Internet Things J.* **2022**, *9*, 9478–9502. [CrossRef]
106. Ahmed, M.U.; Begum, S.; Fasquel, J.-B. *Internet of Things (IoT) Technologies for HealthCare*; Packt Publishing Ltd.: Birmingham, UK, 2018.
107. Aledhari, M.; Razzak, R.; Qolomany, B.; Al-Fuqaha, A.; Saeed, F. Biomedical iot: Enabling technologies, architectural elements, challenges, and future directions. *IEEE Access* **2022**, *10*, 31306–31339. [CrossRef]
108. Mehdiabadi, A.; Shahabi, V.; Shamsinejad, S.; Amiri, M.; Spulbar, C.; Birau, R. Investigating industry 5.0 and its impact on the banking industry: Requirements, approaches and communications. *Appl. Sci.* **2022**, *12*, 5126. [CrossRef]
109. Herrmann, H.; Masawi, B. Three and a half decades of artificial intelligence in banking, financial services, and insurance: A systematic evolutionary review. *Strateg. Change* **2022**, *31*, 549–569. [CrossRef]
110. Kaushal, V.; Balaini, A. E-banking: Challenges and issues. *IOSR J. Bus. Manag.* **2019**, *19*, 69–73.
111. Kalsoom, T.; Ramzan, N.; Ahmed, S.; Ur-Rehman, M. Advances of sensor technologies in the era of smart factory and industry 4.0. *Sensors* **2020**, *20*, 6783. [CrossRef]
112. Hajiheydari, N.; Delgosha, M.S.; Olya, H. Scepticism and resistance to IoMT in healthcare: Application of behavioural reasoning theory with configurational perspective. *Technol. Forecast. Soc. Change* **2021**, *169*, 120807. [CrossRef]
113. Gómez-Valiente, P.; Benedí, J.P.; Lillo-Castellano, J.M.; Marina-Breysse, M. Smart-iot business process management: A case study on remote digital early cardiac arrhythmia detection and diagnosis. *IEEE Internet Things J.* **2023**, *10*, 16744–16757. [CrossRef]
114. Umair, M.; Cheema, M.A.; Cheema, O.; Li, H.; Lu, H. Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT. *Sensors* **2021**, *21*, 3838. [CrossRef] [PubMed]
115. Brous, P.; Janssen, M.; Herder, P. The dual effects of the internet of things (iot): A systematic review of the benefits and risks of iot adoption by organizations. *Int. J. Inf. Manag.* **2020**, *51*, 101952. [CrossRef]
116. Arfi, W.B.; Nasr, I.B.; Kondrateva, G.; Hikkerova, L. The role of trust in intention to use the iot in ehealth: Application of the modified utaut in a consumer context. *Technol. Forecast. Soc. Change* **2021**, *167*, 120688. [CrossRef]
117. Lederman, R.; Ben-Assuli, O.; Vo, T.H. The role of the internet of things in healthcare in supporting clinicians and patients: A narrative review. *Health Policy Technol.* **2021**, *10*, 100552. [CrossRef]
118. Minani, J.B.; Sabir, F.; Moha, N.; Guéhéneuc, Y.-G. A Systematic Review of IoT Systems Testing: Objectives, Approaches, Tools, and Challenges. *IEEE Trans. Softw. Eng.* **2024**, *50*, 785–815. [CrossRef]

119. Pal, D.; Funilkul, S.; Zhang, X. Should i disclose my personal data? perspectives from internet of things services. *IEEE Access* **2021**, *9*, 4141–4157. [CrossRef]
120. Adam, M.; Baroudi, U. Federated Learning for IoT: Applications, Trends, Taxonomy, Challenges, Current Solutions, and Future Directions. *IEEE Open J. Commun. Soc.* **2024**, *5*, 7842–7877. [CrossRef]
121. Makkar, A.; Ghosh, U.; Sharma, P.K.; Javed, A. A fuzzy-based approach to enhance cyber defence security for next-generation iot. *IEEE Internet Things J.* **2023**, *10*, 2079–2086. [CrossRef]
122. Kaur, J.; Kaur, K. A fuzzy approach for an IoT based automated employee performance appraisal. *Tech. Sci. Press* **2017**, *53*, 24–38.
123. Marinkovic, S.; Popovici, E. Network coding for efficient error recovery in wireless sensor networks for medical applications. In Proceedings of the 2009 First International Conference on Emerging Network Intelligence, Sliema, Malta, 11–16 October 2009; pp. 15–20.
124. Jalali, M.S.; Kaiser, J.P.; Siegel, M.; Madnick, S. The internet of things promises new benefits and risks: A systematic analysis of adoption dynamics of iot products. *IEEE Secur. Priv.* **2019**, *17*, 39–48. [CrossRef]
125. Wang, S.; Wan, J.; Zhang, C. Implementing smart factory of industrie 4.0: An outlook. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 3159805. [CrossRef]