The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

Transformation for Quality Business Processes in the Internet of Things: A Comparative Study

Muttappa M. Mantur
Department of Computer Science, Govt. First Grade College for Women and PG Centre, Jamkhandi Karnataka, India
Affiliated to KSAWU, Vijayapura

Abstract

The Internet of Things (IoT) is revolutionising how businesses run and has the potential to significantly enhance best practices. This study compares the transformational effects of IoT on good business practices across a range of industries. This article looks at how IoT is being used in the manufacturing, transportation, healthcare, and supply chain industries and evaluates the degree of transformative influence on each industry and analyses the advantages and difficulties of IoT deployment. The study also looks into how IoT might improve customer satisfaction and quality management procedures. The findings demonstrate that IoT has the ability to drastically alter company procedures and enhance quality control. IoT adoption, however, necessitates thorough planning, infrastructure investment, and attention to security and privacy issues. This offers insightful information about how IoT is transforming good business practices, and it can help companies implement IoT to boost productivity and competitiveness.

Keywords*:* Internet of Things, IoT, quality business practices, manufacturing industry, healthcare industry, comparative study

1. Introduction

The Internet of Things (IoT) is a fast expanding network of linked hardware, software, and sensors that can gather and exchange data online. This technology has the ability to drastically alter how businesses run by allowing them to streamline operations, cut costs, and increase customer happiness. Yet, a focus on good business procedures is necessary for the effective deployment of IoT in the workplace [1]. In this essay, we look at how IoT has affected several industries' high-quality business processes. In order to integrate IoT into their operations and enhance their business processes, companies in a variety of industries, including manufacturing, healthcare, and transportation have taken diverse techniques. In addition, this article gives a thorough study of the difficulties and chances that the Internet of Things (IoT) presents in changing business operations, including the requirement for data security, privacy, and governance. The purpose of this paper is to offer insightful information on how businesses may use IoT to alter their operations and create high-quality business processes. The report provides a comparative analysis by looking at the experiences of various industries, which can aid firms in identifying best practices and avoiding common problems.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

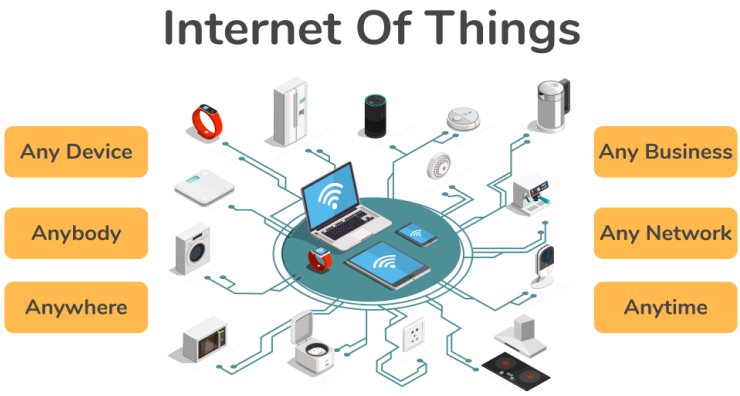

Figure 1: IoT connects machines together from various fields

The proliferation of the Internet of Things (IoT) has given rise to a wide range of unique applications in practically every area of daily life. From 2012 to 2018, the number of IoT devices more than tripled, reaching more than 34 billion [2]. IoT is a network that connects things with unique identifiers to the internet. Through the use of distinctive identification and sensing, data may be gathered about the thing and its state can be modified at any time, from anywhere [3]. Hence, the central concept is the ubiquitous presence of things or items like Radio-Frequency Identification (RFID) tags, sensors, actuators, or mobile phones that may communicate and work together [4].IoT technology is increasingly being used by businesses, particularly industrial ones, for the effective management and control of industrial assets and processes in order to boost productivity and lower operating costs [5]. Because to capabilities like its ability to optimise company processes and real-time communication, IoT has quickly acquired appeal in the business world and become a term. As a result, its applications are regarded to be greatly growing in a variety of domains of endeavour [6]. The idea of IoT has been applied in recent years to telemedicine monitoring, intelligent transportation, smart energy metre reading, and greenhouse monitoring [7].IoT promises to enable worldwide communication by connecting "things" all over the world via small systems and sensor networks. Concerns about security, privacy, and concerns of trust in the transmission of the information are raised as a result [8].

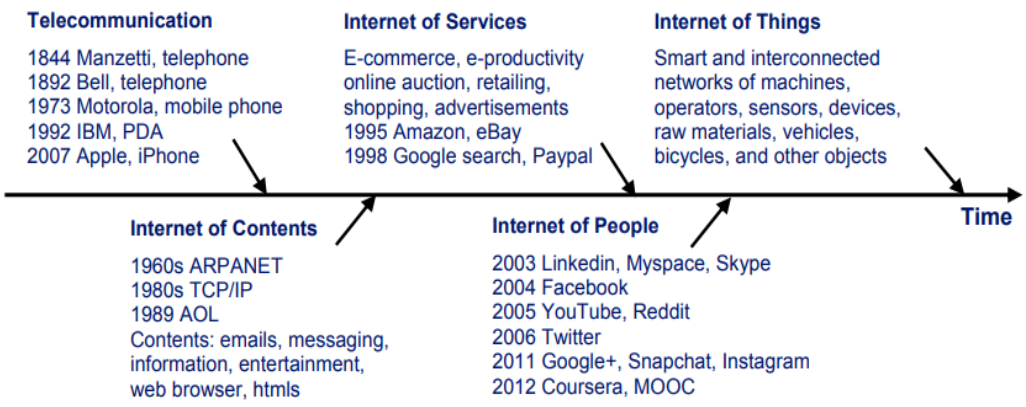

Figure 2: The development of the Internet

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

The combination of this trend with the recent rapid breakthroughs in cloud computing, virtual reality, and big data analytics offers a new paradigm for the transformation of high-quality business operations. In addition, we examined the critical IoT security issues for organisations and operations as well as the worldwide IoT and smart manufacturing regulations put in place to support the creation of the first truly global smart factory. Lastly, the transformation of the IoT for high-quality business processes is examined along with its possibilities, threats, and Strengths. We believe that our study will encourage additional in-depth investigation and cross-disciplinary work to develop Internet of Things (IoT) technology.

2. Literature Review

***2.1 The Internet of Things*:** The Internet of Things (IoT) is an inventive collaboration of various complementary technologies that work together to close the gap between the digital and physical worlds [9, 10]. The Massachusetts Institute of Technology (MIT) Auto-ID Center for SCM members first used the term "Internet of Things" in 1999 to describe a method of tracking items via the Internet using radio-frequency identification (RFID) linking to an Electronic Product Code (EPC) serving as a unique universal identifier for each individual item [11, 12]. Since then, the definition of a "Thing" has expanded to encompass a variety of electronic gadgets (such as RFID tags, sensors, actuators, cellphones, and smart objects) that may be individually identified, read, sensed, located, addressed, and autonomously controlled over the Internet [13, 14].By utilising the Internet as a communication infrastructure, storage mechanism, and medium for data processing and synthesis, it is hypothesised that IoT devices' capabilities would surpass the inherent features of any device [15, 16]. These days, social media, cloud computing, and (big) data analytics all help to further enhance the IoT platform [15]. Self-awareness, individuality, control, interconnection, adaptability, transformability, synergy, self-decisiveness, and strategic behaviour are important IoT characteristics [9, 16]. These attributes and capacities have been expected by academics to help the IoT produce social, economic, and environmental benefits [15, 17].

***2.2 Industry 4.0 and IoT*:** According to various sources [9, 18, and 19], the IoT is a catalyst for the advent of the Industry 4.0 age of automation and digitalization. Industry 4.0 introduces smart products, smart machines, and intelligent services like quality-controlled production, logistics, and maintenance [18], in contrast to the three previous industrial revolutions, which focused on mechanical power (Industry 1.0), mass production (Industry 2.0), and the digital revolution (Industry 3.0). The aura of the Internet of Things (IoT) as one of the most influential technologies has come to light since Germany announced the Industry 4.0 programme in 2011 and was later recognised as a key topic on the 2016 World Economic Forum's agenda [18, 19].Industry 4.0 was created with the intention of taking industrial production to a new level, but its core principles can only be realised if SCs can operate harmoniously by becoming more digital, self-sufficient, and information-led [19, 17]. Thus, Industry 4.0 depends on the integration of logistics activities with Internet-connected technology [18]. Additionally, for major performance gains, the IoT platform supports the integration of supply chain activities with external partners like suppliers and customers [10]. While IoT applications can help with real-time asset tracking, material flow tracking, improved transport handling, and precise risk management in the early Industry 4.0 context, the envisaged potential is a self-sustained supply chain platform through complete automation with little to no human intervention [17].The

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

reliance on discrete data silos, which results in the data not always being immediately available, limits the transfer of SCM to Industry 4.0 [18, 20]. By bridging information gaps through real-time tracking of product flows, information interchange, and automated handling, the IoT, on the other hand, has the ability to turn the SC into an integrated system and facilitate the shift to Industry 4.0 [11, 19, and 17].

***2.3 IoT and supply chain management*:** Industry IoT is not just for big, clever companies and their SCs. It is a widely used technology that plays a variety of roles in SCM [10, 20], including tying information to vendors, gathering real-time progress data from them, giving visibility to parts and raw materials, generating real-time quality/maintenance data, tracking inventory, sharing information, and joint orders, enabling enhanced reverse logistics, and capturing product data while in use [18, 20]. Additionally, sensor technologies are being incorporated into more and more cars. These technologies allow for real-time communication between the car and its surroundings as well as faster speeds and platooning of cars, all of which help to shorten travel times, ease traffic, and expand the capacity of already-existing infrastructure [21]. Real-time data from the Internet of Things is now available, and its analysis enables stakeholders to improve strategic results at the SC and firm levels [5, 22]. In order to improve driver safety, operational effectiveness, and environmental sustainability, for instance, Hopkins and Hawking (2018) demonstrate how IoT and big data analytics are employed in a logistics company.The adoption and utilisation of the IoT face various obstacles despite its potential [23, 24]. Tu (2018) discovers that many businesses are hesitant to invest in the IoT because they are unsure of its potential. Given that technologies are becoming more widespread, subtle, and omnipresent, it is difficult to forecast how digitalization will effect various businesses [25, 26]. Due to social, economical, and technical factors [18], many people are still hesitant to make investments in IoT-related projects, even if the cost of IoT hardware like RFID tags and readers has decreased [12].Integration of logistics activities along supply chains with diverse technologies and data services is one of the key obstacles to adoption [23], along with other crucial hurdles like security, ethics, privacy, and standardisation [16]. Moreover, increased focus on e-waste reduction is required for environmental sustainability [27]. According to Alieva and Haartman (2020), we should focus on reducing e-waste produced by Industry 4.0 automation and explore new business opportunities through reversed logistics. In their review of the literature, Whitmore et al. (2014) divided the barriers into four categories: security, privacy, legal/accountability, and general. These hinder managers from taking advantage of the IoT's potential for visibility [23].Although sharing information has always been difficult in the SC environment, interoperability can help the IoT realise its true potential [18]. All SC partners may benefit from sharing the collected data on a single IoT platform [10]. This subject requires first-person accounts from practitioners who are directly involved in its use because there are conflicting scholarly viewpoints regarding the opportunities and difficulties provided by the IoT in SCM and the recent development of its practical application and study [11,16].

It is critical to comprehend from a practical standpoint how these new smart gadgets connect all channel partners wherever they are, enhance supply chain visibility, and benefit channel partners [28]. Yet, little empirical study has looked at its potentials in the context of SCM, and current scholarship regarding the application of the IoT to SCM hardly ever integrates management and operations perspectives [18, 16, 23, 20, and 14].Kaya (2020) makes an effort to conceptualise the IoT in SCM in a recent work, although others (such as Attaran (2020),

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

Birkel & Hartmann (2019), and Evtodieva et al. (2020) support proof-of-concept via literature studies. IoT efforts are categorised by Caro and Sadr (2019) on an opportunity map that separates them based on their value in decoupling supply and demand in retail; by doing this, they underline that the technology's true potential lies in unforeseen advantages that come with IoT adoption. To further understand these advantages, though, in-depth empirical narratives of IoT adoption and use are needed. Many businesses are still hesitant to fully recognise the value of integrating developing ICT into the supply chain and operational conditions since there is still a lack of proof-of-concept [30].Haddud et al. (2017), who survey academics but suggest crucial directions for future research using open-ended questions with industry practitioners to gain practical insights, have provided limited empirical evidence in the field. In contrast, the literature review by Mishra et al. (2016) asserts the necessity of conducting case studies with grounded theory approach to explain the complexity of IoT integration in SCM.

3. IoT Architecture

The Internet of Things (IoT) architecture refers to the overall design of the network that connects physical devices and appliances to the internet, allowing them to collect and exchange data. There are several layered architectures for IoT [31], ranging from 3 to 7 layers, each with its own benefits and drawbacks. Here's a breakdown of each architecture:

• ***Three-layered IoT Architecture*:** This architecture consists of three layers:

Device layer: This layer consists of IoT devices such as sensors, actuators, and edge devices.

Network layer: This layer is responsible for communication between devices and the cloud. This layer includes gateways, routers, and communication protocols.

Cloud layer: This layer consists of cloud servers and applications that process and store data.

Benefits:

• This architecture is simple and easy to understand.
• Cost-effective.
• Easy to implement.

Drawbacks:

• Data processing and storage are limited to the edge devices.
• There may be a delay in sending data to the cloud.

• ***4-layer Architecture*:** This architecture is similar to the 3-layer architecture, but it includes a fourth layer, called the "Fog" layer, which acts as a bridge between the edge devices and the cloud.

Benefits:

• The fog layer improves data processing and storage capabilities
• It reduces the delay in sending data to the cloud.
• Better decision making based on the processed data

Drawbacks: The fog layer adds complexity and cost to the architecture.

• ***5-layer Architecture*:** This architecture adds another layer, called the "Data Center" layer, between the fog and the cloud. The data center layer is responsible for data storage and management.

Benefits:

• The data center layer provides additional data storage and management capabilities.
• It increases the reliability and security of the system.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

Drawbacks:

- The data center layer adds more complexity and cost to the architecture.

- ***6-layer Architecture*:** This architecture includes an additional layer, the "Security" layer, responsible for ensuring the privacy and security of the data.

Benefits:

- The security layer provides additional protection for sensitive data.

Drawbacks:

- The security layer adds more complexity and cost to the architecture.

- **7-layer Architecture:** This architecture includes an additional layer, the "Application" layer, which provides a user-friendly interface for accessing and controlling the system.

Benefits:

- The application layer makes it easy for users to interact with the system.

Drawbacks:

- The application layer adds more complexity and cost to the architecture.

There are several degrees of abstraction in IoT platforms. The application layer, which is the first layer for users and is where they can control devices and receive data on their smart devices, is followed by the communication layer, where data is transferred using different protocols between the various sensors, actuators, and their local gateways as well as between global gateways, and then comes the physical layer, which contains sensors, actuators, and controllers and their interactions with the gateway [32]. Figure 2 describes high level IoT architecture.

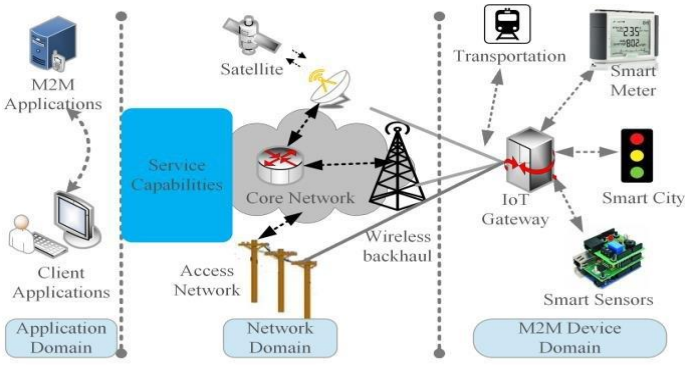

Figure 3: High-level IoT architecture

4. How Iot Is Being Used In The Manufacturing, Transportation, Healthcare, And Supply Chain Industries?

The Internet of Things (IoT) is being used in a variety of businesses to increase productivity, cut costs, and offer customised services and it has been transforming various industries over the years and till now, it continues to make an impact in manufacturing, transportation, healthcare, and supply chain industries. IoT refers to the network of physical devices, vehicles, and other objects embedded with sensors, software, and connectivity, enabling them to exchange data and interact with each other over the internet. This technology has revolutionized the way businesses operate by providing real-time insights into their operations,

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

improving efficiency, reducing costs, and enhancing customer experience. In this context, let's take a closer look at how IoT is being used in the manufacturing, transportation, healthcare, and supply chain industries. We may anticipate even more cutting-edge IoT applications in the years to come as technology develops and In this section, I'll describe how, IoT is employed in the manufacturing, transportation, healthcare, and supply chain sectors:

***4.1 Manufacturing Industry*:** IoT has been used in the manufacturing industry for several years now, and it continues to be a key driver of innovation and efficiency in the sector and it has been transforming the manufacturing industry since its inception. The adoption of IoT in the manufacturing industry started gaining traction in 2015, when companies started using IoT sensors and devices to monitor their machines and products in real-time. Since then, the use of IoT in manufacturing has only increased, with predictive maintenance, inventory management, and quality control being some of the most common applications of IoT in the industry. According to a research report by MarketsandMarkets, "IoT in Manufacturing Market by Component (Solutions (Network Management and Data Management) and Services (Professional and Managed)), Deployment Mode, Organization Size, Application, Vertical (Process and Discrete) and Region - Global Forecast to 2026", the global IoT in Manufacturing Market size to grow from USD 50.0 billion in 2021 to USD 87.9 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 11.9% during the forecast period [33]. IoT is being used in manufacturing for predictive maintenance, inventory management, and quality control, among other things. For instance, Bosch Rexroth, a German manufacturing company, has developed an IoT-enabled predictive maintenance system that uses machine learning to predict when a machine is likely to fail, enabling companies to schedule maintenance proactively.

***4.2 Transportation Industry*:** The use of IoT in transportation started gaining momentum in 2017, with fleet management, route optimization, and safety being the primary applications of IoT in the industry. Since then, the use of IoT in transportation has only increased, with companies using IoT sensors and devices to track the location and condition of vehicles and cargo in real-time, enabling transportation companies to optimize their routes, reduce fuel consumption, and increase safety. For instance, DHL, a global logistics company, has developed an IoT-enabled logistics platform that uses sensors to track shipments and provide real-time visibility into their location and condition. Due to the COVID-19 pandemic, the IoT in transportation market is expected to decile as a result of numerous government, public, and other organizations adopting a work-from-home culture for their personnel. Moreover, a number of government agencies and non-governmental organizations (NGOs) are using IoT in transportation to reduce losses caused by natural disasters, pandemic situations, and to increase their market share. According to a report by Allied Market Research, the global IoT in transportation market size was valued at $83.25 billion in 2020, and is projected to reach $495.57 billion by 2030, registering a CAGR of 19.9% from 2021 to 2030 [34]. The global IoT in transportation market is segmented on the basis of type, mode of transport, application, and region. By type, it is categorized into hardware, software, and services. By mode of transport, it is divided into roadways, railways, airways, and maritime. By application, it is classified into traffic congestion control systems; automotive telematics; reservation, toll, & ticketing systems; security & surveillance systems; remote monitoring; and others. Region wise, it is analyzed across North America, Europe, Asia-Pacific, and LAMEA. The key players operating in the global IoT in transportation industry includes Alcatel-Lucent, AT&T Inc., Garmin

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

International Inc., IBM Corp., Denso Corp., Thales Group, General Electric, Verizon Communications Inc., Cisco Systems, Inc., and TomTom N.V. These players have adopted various strategies to increase their market penetration and strengthen their position in the industry.

***4.3 Healthcare Industry*:** IoT is being used in the healthcare industry for remote patient monitoring, medication management, and disease management. The adoption of IoT in the healthcare industry started gaining traction in 2018. Since then, the use of IoT in healthcare has only increased, with the COVID-19 pandemic accelerating the adoption of remote monitoring technologies. According to a report by ResearchAndMarkets, the global internet of things (IOT) in healthcare market size reached US$ 277.8 billion in 2022. Looking forward, the publisher expects the market to reach US$ 687.5 billion by 2028, exhibiting a CAGR of 16.3% during 2022-2028 [35]. IoT is being used to connect medical devices, wearables, and other health-related products to the internet, enabling healthcare providers to monitor patients' health remotely and provide personalized care. For instance, Philips, a healthcare technology company, has developed an IoT-enabled remote patient monitoring system that uses sensors to track vital signs and alert healthcare providers when a patient's condition requires attention.

***4.4 Supply Chain Industry*:** IoT is being used in the supply chain industry for inventory management, asset tracking, and supply chain optimization. According to a report by Grand View Research, the global supply chain management market size was valued at USD 21,129.2 million in 2022 and is expected to expand at a CAGR of 11.1% from 2023 to 2030. The COVID-19 outbreak had a positive impact on the target market. A significant surge has been observed due to the increased usage of SCM during the COVID-19 pandemic to predict and meet the demand and supply requirements [36]. IoT is being used in various industries to improve efficiency, reduce costs, and provide personalized services. As the technology continues to advance, we can expect to see even more innovative uses of IoT in the years to come.

5. An Evaluation Of The Degree Of Transformative Influence Of Iot On Each Of The Industries

5.1 Manufacturing Industry: IoT has had a transformative influence on the manufacturing industry, enabling companies to improve their operations in many ways. By using IoT for predictive maintenance, inventory management, and quality control, manufacturers can reduce downtime, optimize their inventory levels, and improve product quality. IoT has also enabled manufacturers to connect their machines and production lines, creating a "smart factory" environment where data can be used to optimize processes and increase efficiency. Overall, IoT has enabled the manufacturing industry to become more agile, responsive, and competitive.

***5.2 Transportation Industry*:** IoT has had a transformative influence on the transportation industry, enabling companies to optimize their routes, reduce fuel consumption, and increase safety. By using IoT to track the location and condition of vehicles and cargo in real-time, transportation companies can improve their supply chain management and provide better customer service. IoT has also enabled the development of autonomous vehicles, which have the potential to revolutionize transportation in the future. Overall, IoT has enabled the transportation industry to become more efficient, sustainable, and safe.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

5.3 Healthcare Industry: IoT has had a transformative influence on the healthcare industry, enabling providers to improve patient outcomes and reduce healthcare costs. By using IoT for remote patient monitoring, medication management, and disease management, healthcare providers can deliver more personalized care and detect health issues before they become serious. IoT has also enabled the development of new medical devices and wearables, which can provide patients with continuous monitoring and feedback. Overall, IoT has enabled the healthcare industry to become more patient-centric, efficient, and effective.

5.4 Supply Chain Industry: IoT has had a transformative influence on the supply chain industry, enabling companies to improve their supply chain management and reduce costs. By using IoT for inventory management, asset tracking, and supply chain optimization, companies can better manage their inventory levels, reduce waste, and improve their logistics processes. IoT has also enabled the development of new delivery models, such as drones and autonomous vehicles, which can improve delivery times and reduce transportation costs. Overall, IoT has enabled the supply chain industry to become more responsive, flexible, and efficient.

6. Impact Of Iot On Quality Business Processes In Various Industries

Quality business operations across a range of industries have been significantly impacted by the Internet of Things (IoT). The term "Internet of Things" (IoT) describes a network of interconnected gadgets that are equipped with sensors, software, and other technologies. This enables them to gather and share data with other gadgets on the network as well as with centralised systems. These are a few instances of how IoT has influenced high-quality business processes across diverse industries:

***6.1 Manufacturing*:** IoT has revolutionized the manufacturing industry by enabling predictive maintenance, real-time monitoring, and process optimization. Manufacturers can use IoT sensors to collect data from their production lines, identify areas of inefficiency, and make data-driven decisions to improve their processes. This has led to reduced downtime, increased productivity, and improved product quality.

***6.2 Healthcare*:** IoT has transformed the healthcare industry by enabling remote patient monitoring, predictive analytics, and personalized medicine. Healthcare providers can use IoT devices to collect data on patients' vital signs, medication adherence, and other health metrics. This data can be used to identify patterns and predict health outcomes, allowing providers to intervene before a patient's condition deteriorates.

***6.3 Agriculture*:** IoT has improved the efficiency and sustainability of agriculture by enabling precision farming. Farmers can use IoT sensors to collect data on soil moisture, nutrient levels, and weather conditions. This data can be used to optimize irrigation, fertilization, and pest control, reducing waste and increasing yields.

6.4 Logistics: IoT has revolutionized the logistics industry by enabling real-time tracking and predictive analytics. Logistics companies can use IoT sensors to track the location and condition of their shipments, optimize their routes, and predict delivery times. This has led to improved efficiency, reduced costs, and better customer service.

6.5 Retail: IoT has transformed the retail industry by enabling personalized marketing, inventory management, and customer engagement. Retailers can use IoT sensors to collect data on customers' preferences, buying habits, and in-store behavior. This data can be used to

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

personalize marketing campaigns, optimize inventory levels, and create more engaging in-store experiences.

7. The Different Approaches Used By Businesses In Different Sectors

The study compares the approaches used by businesses in different sectors, such as manufacturing, healthcare, and transportation, to incorporate IoT into their operations and improve their business processes.

***7.1 Manufacturing*:** In the manufacturing sector, IoT technology is being used to optimize production processes, reduce waste, and increase efficiency. Manufacturers are incorporating sensors and other IoT devices into their production lines to gather data on performance and identify areas for improvement. This data is then used to adjust processes, reduce downtime, and improve product quality.

- Sensors and IoT-enabled devices to monitor and control machines and equipment in real-time, optimize production processes, and prevent downtime.
- Asset tracking and management systems to monitor the location, condition, and performance of equipment and assets.
- Predictive maintenance systems that use machine learning algorithms and sensor data to predict when machines and equipment will need maintenance.

7.2 Healthcare: In the healthcare sector, IoT technology is being used to improve patient care and reduce costs. IoT devices such as wearables, smart pills, and remote patient monitoring systems are being used to collect data on patient health and behavior. This data is then analyzed to identify trends and develop personalized treatment plans.

- Wearables and remote patient monitoring devices that track patient health metrics such as heart rate, blood pressure, and glucose levels.
- Smart pills that contain sensors that monitor medication adherence and provide real-time data on the patient's response to medication.
- IoT-enabled medical equipment that provides real-time data on patient vitals and alerts medical staff of any abnormalities or emergencies.

7.3 Transportation: In the transportation sector, IoT technology is being used to improve logistics and reduce costs. Sensors and other IoT devices are being used to track the location and condition of goods in transit. This data is then used to optimize delivery routes, reduce transportation costs, and improve customer satisfaction.

- GPS tracking and telematics devices that provides real-time data on the location, speed, and condition of vehicles and cargo.
- Sensors and IoT-enabled devices that monitor the temperature, humidity, and other environmental conditions of goods in transit.
- Predictive maintenance systems that use machine learning algorithms and sensor data to predict when vehicles and equipment will need maintenance.

8. Security Threats of IoT

By considering the following five principles when designing and implementing IoT systems, businesses and individuals can ensure that their IoT devices and data are secure and protected from various security threats.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

8.1 **Confidentiality:** In the digital world, confidentiality refers to safeguarding user identities and preventing outside interference. By gaining illegal access to private user information using a variety of means, confidentiality risks typically violate the privacy of users [37]. Another breach of confidentiality is the unintentional disclosure of sensitive information [38]. Confidential data transmission to nearby nodes or data transmission to an unauthorised user pose a danger to confidentiality for IoT-based devices [39]. Every device and sensor in the IoT network has the danger of a possible confidentiality violation. Due to the possible hazards that any subpar encryption method or backdoor access flaws provide to the data secrecy of several users on a network, these issues could have very negative effects [40].

8.2 **Integrity**: In order to maintain the data's credibility and correctness, the integrity of the information must be protected from cybercriminals and errors that may occur during transmission and reception. Information could be changed by malicious users while it is in the transmission medium [40]. The transmission of information can also be significantly impacted by channel imperfections, electromagnetic interference, and instrument limits. The integrity of data in IoT devices can only be preserved when the authorised user accesses it over a secure interface and a secure medium [41].

8.3 **Availability*:*** Data accessibility ensures that authorised users have rapid access to information resources. Data delivery whenever needed in both everyday circumstances and emergency scenarios is one of the key objectives of IoT services [42]. One of the main objectives of IoT service providers is to provide immediate data availability because large organisations frequently utilise IoT services to access massive amounts of data. The main availability threats for IoT services that might obstruct information flow and deny data to end users are denial of service attacks and bottleneck situations [43].

8.4 **Authenticity*:*** Giving only legitimate users access to the network is connected to authenticity. Threats to authentication revolve around changing control settings and gathering data that can be exploited to get unauthorised access to sensitive information. The data can be accessed, modified, or even deleted by an unauthorised user, which compromises the data's integrity [37]. IoT authentication vulnerabilities are mostly brought on by improper authentication mechanisms, tag cloning, RFID eavesdropping, and spoofing. A breach in authentication at the administrative level can also jeopardise the entire network by blocking access to authorised users, stealing critical data, flooding the network, and other things [40].

8.5 **Non-Repudiation*:*** In order to access the offered service, a legitimate person must be authenticated in accordance with non-repudiation. This hazard is connected to the autonomy, pervasiveness, and ubiquity of the Internet of Things. An crucial component of the Internet of Things that offers reliable communication is the link between authentication and non-repudiation. Attacks on this aspect of the IoT environment include connection loss, resource limitations, and resource and energy waste. The defence against fake message acknowledgment receipt is jeopardised by this attack [44, 45].

9. Set Of Security Requirements Required to Make IoT Secure- Empirical Analysis

IoT (Internet of Things) device security is essential for preventing security lapses and safeguarding sensitive data. Many security standards must be met in order to accomplish this. To make IoT secure, a set of security requirements must be met. These specifications cover physical security, network security, data security, application security, device security, data

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

level security, and user education. IoT networks and devices can be made more secure and less susceptible to security breaches by complying with these guidelines. The empirical analysis of previous studies on security and privacy issues in the IoT context is presented in this part. The studies are comprehensively reviewed in Table 1.

TABLE-I
SET OF SECURITY REQUIREMENTS REQUIRED TO MAKE IOT SECURE- EMPIRICAL ANALYSIS

Author name and year	Aim of paper	Findings
Babar et. al., (2010)[43]	This paper aims to provide an overview, investigation and classification of various security and privacy issues associated with IoT.	This study proposed a cube structured model for converging security, privacy and trust in IoT environment
Weber (2010)[37]	The main aim of this study is to assess IT-security-legislation and provisions for the use of IoT	This study had discussed new regulatory approaches for IoT, ensuring privacy and security. This study emphasizes that data authenticated, interception of attacks have to be intercepted, access controlled, and privacy protection of user are essential for IoT.
Zhuo& Chao (2011)[46]	The main aim of this study is to address the vital challenge of supporting multimedia applications in IoT in a secure manner.	A multimedia traffic analysis and method was proposed to securely handle heterogeneity in diverse applications. The proposed model had good trade-off between system efficiency and
Suoa et. al., (2012)[42]	The aim of this study was to deeply analyze security characteristics and architecture of IoT.	This study had outlined key security challenges and had discussed the status of main security technologies such as encryption, safe
Kozlov, Veijalainen & Ali (2012)[40]	This study had analyzed the Security, privacy and trust infrastructure in both bottom-up and top-down construction approaches.	This paper had presented a layered view on the threats related to security, privacy and trust architecture. It had also reviewed EU legislation in privacy and security area and its importance for IoT domain.
Keoh, Kumar & Hannes (2014)[47]	This paper aims to provide an on standardization of the security solutions for IoT ecosystem.	This study had a detailed review on various communication security solutions in IoT and had proposed the use of Constrained Application
Abomhara & Koien (2014)[48]	This study had analysed the current issues related to security and privacy in IoT	This study had revealed that accuracy, confidentiality, integrity, authentication, and access control are the vital for enabling credibility, security, and privacy economically and effectively in IoT environment.
Alqassem(2014)[49]	This study had analyzed privacy and security requirements in IoT	This study had presented a methodological framework to meet the the privacy and security requirements in IoT and this model had proposed to tackle such threats at the earliest stages.
Xu, Wendt &Potkonjak (2014)[50]	The main aim was to conduct a survey study for analyzing security challenges and opportunities with IoT.	This study had analyzed various IoT security protocols and proposed a hardware-based approach. This study had provided a starting-points in developing CAD based security solutions.
Lin & Bergmann (2016)[41]	This study had analyzed privacy and security concerns related to IoT in smart home environment	This paper had recognized two main auto-management technologies for enhancing system security namely autoconfiguration and automatic updating of software and firmware for secure operations. This study also highlighted need for efficient security policies and methods for maintaining automation.
Zhou et. al., (2017)[51]	This study presented challenges related to security and privacy in cloud-based IoT	This study had analyzed both practical and academic requirements in cloud-based IoT and had proposed a novel effective privacy-preserving method for achieving secure data collection from multiple heterogeneous users.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

10. A Case Study- The transformation of BMW Group's Dingolfing plant in Germany [53, 54 and 55]

Industries 4.0 and 5.0 have brought about a significant transformation in business processes, especially in the Internet of Things (IoT). IoT refers to the network of physical objects, devices, vehicles, and other items embedded with sensors, software, and network connectivity that enable them to collect and exchange data. The integration of IoT with Industry 4.0 and 5.0 has allowed for increased automation, efficiency, and productivity in various industries.

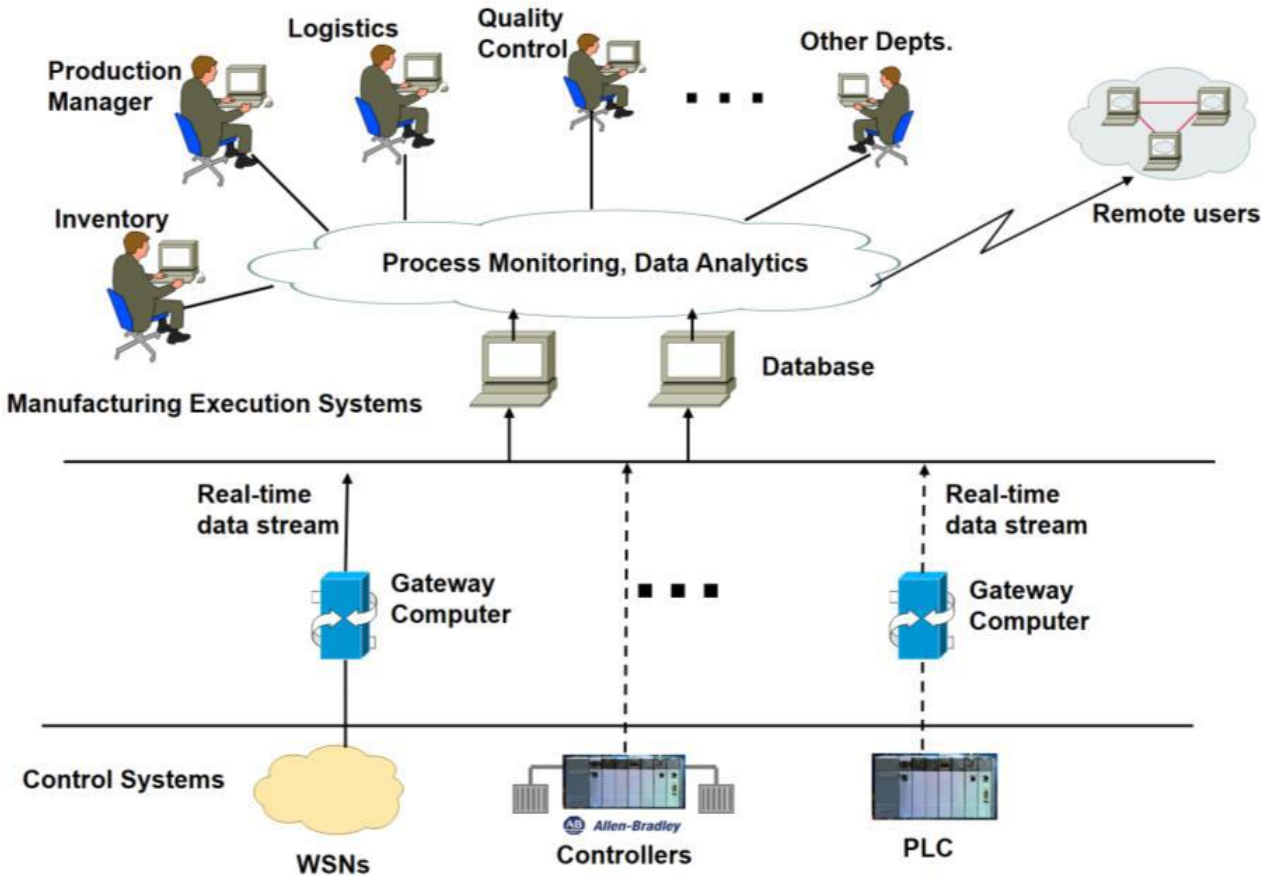

Figure 4: The structure of a manufacturing execution system

Using a manufacturing execution system (MES), Figure 4 depicts one with a typical structure. Between machines, controllers, and the management divisions in manufacturing workplaces, transparent data sharing and information interchange is the goal of MES [44]. Many proprietary control systems, including WSNs, PLCs, and CNC controllers, are available at the process levels from a variety of suppliers. From the bottom layer's control systems, gateway computers transfer real-time data streams to two database servers. Users at the management level then employ software programmes for data analytics and process monitoring.

The MES acts as the foundational system for supply chain optimisation, cost analysis, cost management, and digital performance management. The architecture of current MES systems has recently undergone major alterations as a result of IoT technology. MES is migrating to cloud platforms with the MTConnect protocol and IoT-enabled control systems. The challenge of decoding real-time data streams with proprietary definitions is eliminated by cloud-based MES systems, making data exchange, storage, analytics, and reporting considerably simpler to adopt.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

The case study of transformation for quality business processes in the IoT (Industry 4.0) can be seen in the automotive industry, where businesses are increasingly leveraging Industry 4.0 technologies to optimize their production processes and enhance product quality. One such example is the transformation of BMW Group's Dingolfing plant in Germany. The BMW Group is a well-known producer of high-end automobiles, and its factory in Dingolfing produces a number of BMW models, including the 5 Series, 7 Series, and 8 Series. The business opted to implement Industry 4.0 technology to streamline its manufacturing procedures and raise product quality in order to uphold its high standards of quality and satisfy client needs. The business used an Industry 4.0 solution that feeds data from the production line to a central system via IoT sensors. The system then uses sophisticated analytics and machine learning algorithms to analyse the data in order to find potential quality problems and improve the production process. With the help of the technology, which offers real-time insights into the production process, the business is able to identify flaws early on and stop them before they affect customers. BMW claims that by implementing the solution, productivity has increased by 5%, energy use has decreased by 10%, and defect rates have decreased by 30%. The organisation has noted increased employee satisfaction as a result of workers having better access to information about the production process and more freedom to make decisions based on current data. The BMW Group has deployed Industry 4.0 technologies at other factories throughout the world with equal success, in addition to the advantages obtained at the Dingolfing plant.

In order to optimise its manufacturing processes across all of its plants, the corporation has built a network of connected, smart factories that share data. The BMW Group's successful adoption of Industry 4.0 technology has not gone unnoticed, as seen by the numerous honours and accolades the business has received. The German business publication Wirtschaftswoche named BMW Group the "Most Innovative Business in Germany" in 2019, while the Dingolfing facility won the "Factory of the Year" award in the Large-Scale Production category. BMW claims that the use of the Industry 4.0 solution has decreased the likelihood of product recalls, enhanced quality control by 80%, and increased manufacturing efficiency by 5%. The solution has made it possible for staff to concentrate on more worthwhile duties, like quality assurance and problem-solving, which has increased employee engagement and job satisfaction, according to the organisation.

Overall, the implementation of Industry 4.0 technologies has enabled BMW to enhance its competitiveness in the market by improving its product quality, production efficiency, and customer service. The Dingolfing plant is now recognized as one of the most advanced and efficient automotive production facilities in the world.

11. Swot Analysis

SWOT analysis of IoT in concern to the approaches used by businesses in different sectors, such as manufacturing, healthcare, and transportation, to incorporate IoT into their operations and improve their business processes. IoT has a lot of promise and advantages, but it also faces a lot of obstacles as it develops and enters the market. Hence, in this section, a SWOT analysis is provided. Table-II summarizes the SWOT analysis points.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

TABLE-II
SWOT ANALYSIS FOR TRANSFORMATION FOR QUALITY BUSINESS PROCESSES IN THE IOT

SECTOR	STRENGTHS	WEAKNESSES
IoT in Manufacturing	Improved efficiency and productivity through real-time monitoring and predictive maintenance. Cost savings through automation of processes and reduction in downtime. Better supply chain management and inventory control.	High initial investment cost for implementation. Complex data management and security challenges. Resistance to change and lack of skilled workers.
IoT in Healthcare	Improved patient outcomes through remote monitoring and early detection of health issues. Enhanced patient engagement and communication with healthcare providers. Streamlined workflows and reduced administrative burden.	Privacy and security concerns regarding patient data. Reliance on internet connectivity and potential for system failure. Limited interoperability between different IoT devices and systems.
IoT in Transportation	Improved safety through real-time monitoring and predictive maintenance of vehicles. Optimization of logistics and supply chain management. Increased efficiency and reduced costs through automation of processes.	Security concerns regarding IoT devices and data. The need for high-speed internet connectivity and potential for system failure. The need for standardization and interoperability among different IoT devices and systems.
SECTOR	**OPPORTUNITIES**	**THREATS**
IoT in Manufacturing	Integration of IoT with AI and machine learning to further improve automation and predictive maintenance. Increased use of wearables for employee safety and monitoring. The rise of Industry 4.0 and the need for digital transformation.	Cybersecurity risks and potential data breaches. Dependency on internet connectivity and the potential for system failure. The need for skilled workers to manage and maintain IoT systems.
IoT in Healthcare	Increased use of wearables and remote monitoring devices for chronic disease management. The use of IoT in telemedicine and virtual care. The integration of AI and machine learning to analyze patient data and provide more personalized treatment	Regulatory compliance and potential legal issues. Resistance to change among healthcare providers and patients. The potential for data overload and challenges in managing and interpreting large amounts of patient data
IoT in Transportation	Increased use of IoT in autonomous vehicles and connected infrastructure. The integration of IoT with AI and machine learning to further improve efficiency and safety. The development of smart cities and the use of IoT to improve urban transportation.	Regulatory compliance and potential legal issues. Resistance to change among traditional transportation companies. The need for skilled workers to manage and maintain IoT systems.

12. Conclusion

The Internet of Things (IoT), which is the integration of common gadgets with network access, enables them to gather, analyse, and share data, was the subject of the study piece that examined how it has affected business processes. The study found that integrating IoT technology into business operations has a number of advantages, including better productivity, enhanced customer satisfaction, and higher revenue. For example, IoT can automate routine tasks, monitor customer behavior, and provide insights to improve decision-making. Yet, the study also identified a number of barriers to IoT adoption. IoT devices frequently collect sensitive data that must be safeguarded against hacker assaults and data breaches, making data security and privacy issues one of the key challenges. Lack of standardisation and interoperability is another concern because IoT devices frequently use multiple operating systems, which can cause compatibility problems.

The Ciência & Engenharia - Science & Engineering Journa
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2469 - 2487

The paper emphasised the significance of taking a strategic approach to IoT adoption, including creating an adoption plan, attending to security and privacy issues, and making investments in staff training and development. Additionally, the study recommended that governments should encourage the adoption of IoT by creating policies and legislation that do so while addressing issues with data security and privacy.

13. References

[1] Sofian, S., Shah, M. H., & Rahman, A. (2021). Transformation for Quality Business Processes in the Internet of Things: A Comparative Study. IEEE Access, 9, 103831-103846. doi: 10.1109/ACCESS.2021.3107657.

[2] Burhan, M., Rehman, R., Khan, B., Kim, B.: IoT elements, layered architectures and security issues: A comprehensive survey. Sensors 18(9), 2009.

[3] Minerva, R., Biru, A., Rotondi, D.: Towards a definition of the Internet of Things (IoT). IEEE. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, accessed: 23/11/2020.

[4] Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey. Computer Networks, 54(15), pp. 2787-2805, 2010.

[5] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., Gidlund, M.: Industrial Internet of Things: Challenges, Opportunities, and Directions. IEEE Transactions on Industrial Informatics, 14(11), pp. 4724-4734, 2018.

[6] L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE, 2015.

[7] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.

[8] E. Oriwoh, H. M. al-Khateeb, and M. Conrad, "Responsibility and Non-repudiation in resourceconstrained Internet of Things scenarios," in Conference: Conference: International Conference on Computing and Technology Innovation, 2015.

[9] Balaji, M & Roy, SK. (2017), Value co-creation with Internet of things technology in the retail industry, Journal of Marketing Management, 33(1-2), pp. 7-31.

[10] de Vass, T, Shee, H & Miah, SJ. (2018), The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective, Australasian Journal of Information Systems, 22, pp. 1-19.

[11] Birkel, HS & Hartmann, E. (2019), Impact of IoT challenges and risks for SCM, Supply Chain Management: An International Journal, 24(1), pp. 39-61.

[12] Tu, M. (2018), An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management-a mixed research approach, The International Journal of Logistics Management, 29(1), pp. 131-51.

[13] Mishra, D, Gunasekaran, A, Childe, SJ, Papadopoulos, T, Dubey, R & Wamba, SF. (2016), Vision, applications and future challenges of Internet of Things, Industrial Management & Data Systems, 116(7), pp. 1331-1355.

[14] Atzori, L, Iera, A & Morabito, G. (2010), The Internet of Things: A survey', Computer Networks, 54(15), pp. 2787-805.

[15] Borgia, E. (2014), The Internet of Things vision: Key features, applications and open issues, Computer Communications, 54, pp. 1-31.

[16] Evtodieva, T, Chernova, D, Ivanova, N & Wirth, J. (2020), The Internet of Things: Possibilities of Application in Intelligent Supply Chain Management, in Digital Transformation of the Economy: Challenges, Trends and New Opportunities, Springer, pp. 395-403.

[17] Manavalan, E & Jayakrishna, K. (2018), A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements, Computers & Industrial Engineering, 127, pp. 925-53.

[18] Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019), Internet of things and supply chain management: a literature review, International Journal of Production Research, 57(15-16), pp. 4719-4742.

[19] Hofmann, E & Rüsch, M. (2017), Industry 4.0 and the current status as well as future prospects on logistics, Computers in Industry, 89, pp. 23-34.

[20] Kaya, SK (2020), Industrial Internet of Things: How Industrial Internet of Things Impacts the Supply Chain, Internet of Things (IoT) Applications for Enterprise Productivity, IGI Global, pp. 134-55.

[21] Kshirsagar, P. R., Reddy, D. H., Dhingra, M., Dhabliya, D., & Gupta, A. (2022b). Detection of Liver Disease Using Machine Learning Approach. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 1824–1829. IEEE.

[22] Hopkins, J & Hawking, P. (2018), Big Data Analytics and IoT in logistics: a case study, International Journal of Logistics Management, 29 (2), pp. 575-91.

[23] Büyüközkan, G & Göçer, F. (2018), Digital Supply Chain: Literature review and a proposed framework for future research, Computers in Industry, 97, pp. 157-77.

[24] Haddud, A, DeSouza, A, Khare, A & Lee, H. (2017), Examining potential benefits and challenges associated with the Internet of Things integration in supply chains, Journal of Manufacturing Technology Management, 28(8), pp. 1055-85.

[25] Veeraiah, V., Pankajam, A., Vashishtha, E., Dhabliya, D., Karthikeyan, P., & Chandan, R. R. (2022). Efficient COVID-19 Identification Using Deep Learning for IoT. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 128–133. IEEE.

[26] Whitmore, A, Agarwal, A & Da Xu, L. (2014), The Internet of Things—A survey of topics and trends, Information Systems Frontiers, 17(2), pp. 261-74.

[27] Attaran, M. (2020), Digital technology enablers and their implications for supply chain management, Supply Chain Forum: An International Journal, pp. 1-15. DOI: 10.1080/16258312.2020.1751568

[28] Kenney, M, Rouvinen, P, Seppälä, T & Zysman, J. (2019), Platforms and industrial change, Industry and Innovation, 26(8), pp. 871-9.

[29] Alieva, J & Haartman, R (2020), Digital Muda-The New Form of Waste by Industry 4.0, Operations and Supply Chain Management: An International Journal, 13(3), pp. 269-78.

[30] Sharma, A & Khanna, P. (2020), Relevance of Adopting Emerging Technologies in Outbound Supply Chain: New Paradigm for Cement Industry, Operations and Supply Chain Management: An International Journal, 13(2), pp. 210-21.

[31] Caro, F & Sadr, R. (2019), The Internet of Things (IoT) in retail: Bridging supply and demand', Business Horizons, 62(1), pp. 47-54.

[32] Huddiniah, E & ER, M. (2019), Product Variety, Supply Chain Complexity and the Needs for Information Technology: A Framework Based on Literature Review, Operations and Supply Chain Management: An International Journal, 12(4), pp. 245-55.

[33] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, 2013.

[34] Kapoor, Amita. Hands-On Artificial Intelligence for IoT : Expert Machine Learning and Deep Learning Techniques for Developing Smarter IoT Systems, Packt Publishing, Limited, 2019. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/inflibnet-ebooks/detail.action?docID=5675583.

[35] https://www.marketsandmarkets.com/Market-Reports/iot-manufacturing-market-129197408.html

[36] IoT in Transportation Market: Global Opportunity Analysis and Industry Forecast, 2021–2030, Published Date: Feb 2022, Pages : 250. https://www.alliedmarketresearch.com/IoT-in-transportation-market

[37] INTERNET OF THINGS IN HEALTHCARE MARKET: GLOBAL INDUSTRY TRENDS, SHARE, SIZE, GROWTH, OPPORTUNITY AND FORECAST 2023-2028: https://www.researchandmarkets.com/reports/5732331/internet-things-in-retail-market-global-industry#rela0-5743081

[38] Supply Chain Management Market Size, Share & Trends Analysis Report By Component (Solution, Services), By Deployment, By Enterprise Size, By Vertical, By Region, And Segment Forecasts, 2023 – 2030: https://www.grandviewresearch.com/industry-analysis/supply-chain-management-market-report

[39] R. H. Weber, “Internet of Things – New security and privacy challenges,” Elsevier, 2010.

[40] Kshirsagar, P. R., Reddy, D. H., Dhingra, M., Dhabliya, D., & Gupta, A. (2022a). A Review on Comparative study of 4G, 5G and 6G Networks. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 1830–1833. IEEE.

[41] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.

[42] M. U. Farooq, M. Waseem, and A. Khairi, “A Critical Analysis on the Security Concerns of Internet of Things (IoT),” Int. J. Comput. Appl., vol. 111, no. 7, 2015.

[43] D. Kozlov, J. Veijalainen, and Y. Ali, “Security and Privacy Threats in IoT Architectures,” 2012.

[44] H. Lin and N. W. Bergmann, “IoT Privacy and Security Challenges for Smart Home

[45] Environments,” MDPI, 2016.

[46] H. Suoa, J. Wana, C. Zoua, and J. Liua, “Security in the Internet of Things: A Review,” in International Conference on Computer Science and Electronics Engineering, 2012.

[47] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT),” Springer-Verlag Berlin Heidelb., 2010.

[48] E. Oriwoh, H. M. al-Khateeb, and M. Conrad, “Responsibility and Non-repudiation in resourceconstrained Internet of Things scenarios,” in Conference: Conference: International Conference on Computing and Technology Innovation, 2015.

A. Cooper, “Security for the Internet of Things,” KTH ROYAL INSTITUTE OF TECHNOLOGY SCHOOL OF COMPUTER SCIENCE AND COMMUNICATION (CSC), 2015.

[49] L. Zhou and H.-C. Chao, “Multimedia Traffic Security Architecture for the Internet of Things,” IEEE Netw., 2011.

[50] S. L. Keoh, S. S. Kumar, and H. Tschofenig, “Securing the Internet of Things: A Standardization Perspective,” IEEE Internet Things J., vol. 1, no. 3, pp. 265–275, Jun. 2014.

[51] M. Abomhara and G. M. Koien, “Security and privacy in the Internet of Things: Current status and open issues,” in 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014, pp. 1–8.

[52] Alqassem, “Privacy and security requirements framework for the internet of things (IoT),” in Companion Proceedings of the 36th International Conference on Software Engineering - ICSE Companion 2014, 2014, pp. 739–741.

[53] T. Xu, J. B. Wendt, and M. Potkonjak, “Security of IoT Systems: Design Challenges and Opportunities,” IEEE, 2014.

[54] Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.

[55] d. U. Saenz, A. Artiba and R. Pellerin, "Manufacturing execution system – a literature review," Production Planning & Control, vol. 20, no. 6, pp. 525-539, 2009.

[56] BMW Group. (2021). The Dingolfing Plant. Retrieved from https://www.bmwgroup-plants.com/dingolfing/en.html

[57] PwC. (2019). Industry 4.0: Building the digital enterprise. Retrieved from https://www.pwc.com/gx/en/industries/industry-4.0/landing-page/industry-4.0-building-the-digital-enterprise-april-2019.pdf

[58] The Manufacturer. (2019). BMW's Dingolfing plant showcases digital factory innovation. Retrieved from https://www.themanufacturer.com/articles/bmws-dingolfing-plant-showcases-digital-factory-innovation/