Journal of Information Systems and Informatics

Vol. 6, No. 2, June 2024 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

DOI: 10.51519/journalisi.v6i2.738 Published By DRPM-UBD

The Future of Things: A Comprehensive Overview of Internet of Things History, Definitions, Technologies, Architectures, Communication and beyond

Ofaletse Mphale[1], Karikoga Norman Gorenjena[2], Olebogeng Nojila[3]

[1,2,3] Department of Economics and Management Sciences, North-West University, Mahikeng Campus, South Africa
Email: [1]ofaletse_offie@hotmail.com, [2] koga.gorejena@nwu.ac.za, [3]22646892@nwu.ac.za

Abstract

This paper explores the multifaceted world of IoT, exploring its historical evolution, core definitions, enabling technologies, architectural considerations, communication models and future predictions. Moreover, the paper critically scrutinises the potential benefits and challenges associated with IoT adoption. This study employed a systematic literature review (SLR) methodology to review existing literature between January 2020 and January 2024 on IoT technology. 20 relevant studies out of an initial pool of 45,312 studies were reviewed. The study followed the established Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) framework to ensure a rigorous and unbiased selection process. Findings revealed the lack of a universally accepted definition for IoT and significant variations in architectural models across scholarly works. Moreover, the study acknowledges the complex and ever-evolving nature of IoT technology, recognising its early stages of development. This dynamic technological landscape calls for continuous exploration of future research. Findings will provide valuable insights for academics, researchers, and industry professionals interested in the understanding the intricate technical landscape of IoT and its development. Moreover, by providing insights into growth predictions, benefits, and existing challenges, this will empower stakeholders to navigate the evolving IoT landscape and contribute to its future progress.

Keywords: Internet of Things, IoT Evolution, IoT Architectures, IoT Communication, Sensors

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a dominant trend in recent years, shaping the landscape of 4th generation (4G) technologies. It promises seamless interconnection between uniquely identifiable smart objects and devices within the internet infrastructure [1]. While the term "IoT" has gained significant traction recently, the underlying concept has roots in earlier inventions. Some trace its origins back to the 19th century telephone, but a more relevant starting point is likely the 1990s [2]. Despite ongoing debate about the exact definition, IoT generally refers to a network of physical devices equipped with sensors and software, enabling them to collect and communicate with each other[3], creating a smart and interconnected environment [4]. The key technologies that enable IoT include Radio Frequency Identification (RFID), Near Field Communication (NFC), Wireless Sensor Networks (WSNs), low-energy Bluetooth, low-energy wireless, low-energy radio protocols, and Long-Term Evolution-Advanced (LTE-A) [5]. These technologies provide the specific networking capabilities required for an IoT system, which differs from a standardised network of conventional systems. The IoT architecture serves as the underlying framework that enables communication between internet-connected devices. It encompasses multiple components, including layers, sensors, protocols, actuators, and cloud services [6]. There are four main communication models that dominate the IoT landscape namely; request-response model, publish-subscribe model, push-pull model, and exclusive-pair model [7]. These communication models define how IoT devices initiate contact, establish connections, and exchange information. This enables seamless communication, real-time data collection, and ultimately, the intelligent functionality that defines the IoT [8].

In recent years, the IoT has experienced a surge in growth, rapidly transforming the global landscape. This transformation is driven by an exponential increase in the number of interconnected devices [9]. Forecasts predict a staggering number of connected devices – exceeding 50 billion globally by 2025 [10] – translating to a multi-trillion-dollar market by 2030 [11]. This surge promises immense economic impact, revolutionising businesses through increased productivity, efficiency, and innovation [12]. Experts warn that companies who fail to embrace IoT risk falling behind competitors [32]. Nonetheless, despite these IoT advancements, a crucial gap remains in our comprehensive understanding of its current landscape and technical features. This is evident in several ways. For instance, there is a lack of consensus on a single, universally accepted definition of IoT, leading to subjectivity and ambiguity [13]. Secondly, the absence of a standardised design is reflected in the multitude of proposed architectures by researchers [14]. This inconsistency in understanding the core aspects and boundaries of the IoT landscape hinders the development of a unified view of its current state. To address this knowledge gap, a more rigorous approach is necessary.

This study aims to fill a crucial knowledge gap by employing a systematic literature review (SLR) adhering to the established Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) guidelines. This methodology ensures a more rigorous, objective and transparent evaluation of existing research compared to traditional literature reviews [15]. The study will offer a thorough analysis of the IoT features and landscape, encompassing its history, definition, enabling technologies, architectures, communication models, standards, future growth predictions, applications, potential benefits, and existing challenges. Findings will provide valuable insights for academics, researchers, and industry professionals interested in the understanding the intricate of IoT technical landscape and its development. Moreover, by providing insights into IoT applications, growth predictions, benefits, and existing challenges, this empowers stakeholders to navigate the evolving IoT landscape and can contribute meaningfully to its future development.

2. METHODS

2.1. The Systematic Review Methodology

This study employed a SLR methodology following the established PRISMA guidelines to explore various topics related to the current state-of-the-art IoT features and trends. We begin by outlining the main research question and any sub-questions that guide our investigation.

2.1.1. The main research question

This study aims to understand the current state of knowledge regarding IoT technical features and the overall IoT landscape. This includes its history, core definition, enabling technologies, architectures, communication models, standards and protocols, applications, and predictions for its future growth. Moreover, the study also aims to examine the potential benefits and existing challenges of IoT adoption. Hence, the primary research question is:

"How can a comprehensive analysis of the Internet of Things ecosystem, including its evolution, definitions, architectures, communication protocols, applications, and future trends, alongside potential benefits and challenges, inform our understanding of the current state of IoT landscape?"

2.1.2. The sub-research questions

To address the main research question, this review processes focused on the following sub-research questions:

1) How did the concept of the IoT evolve, and what are the key milestones in its development?
2) How do different scholars define IoT?
3) What are the core technologies that enable IoT functionality?
4) What is the different design architectural models used in IoT systems?
5) What are the most common standards and protocols used in IoT systems?
6) What are the common application areas for IoT across different sectors?

7) What are the forecasted trends for IoT adoption and user base growth in different sectors?
8) What are the key benefits and challenges associated with IoT adoption across different sectors?

Using the PRISMA protocol, we conducted a rigorous search process involving several key phases. This included defining clear inclusion and exclusion criteria to identify relevant studies. Primarily, we focused our search on reputable academic databases such as Scopus, Web of Science, IEEE Xplore, ProQuest, the University of Botswana Library catalogue, and Google Scholar. By formulating effective search strategies, we aimed to retrieve a comprehensive set of research articles, books, conference proceedings, and existing literature reviews from relevant fields like Business Information Systems, Knowledge Management, Information Systems, Computer Information systems, Information Technology, and Computer Science.

The PRISMA method ensures a meticulous and transparent approach throughout the review process [15]. This multi-phased approach, including screening retrieved studies for eligibility, minimises potential bias and enhances the robustness of the review [16]. By carefully considering all relevant and high-quality articles, we aim to ensure the credibility and trustworthiness of our findings. The initial search yielded a total of 45,312 articles and conference proceedings potentially relevant for inclusion. Table 1 provides an overview of the key phases involved in the systematic literature search process.

Table 1. The literature review process adopted by the study

Stage	**Description**
Inclusion criteria	1) Only peer-reviewed research articles, books and conference proceedings. 2) Studies published between January 2020 and January 2024. However, some earlier studies which are highly influential were considered. 3) Only English-language publications were considered. 4) Only studies focusing on IoT adoption
Exclusion criteria	1) Studies not published in full text in academic journals or conference proceedings. 2) Studies with titles and abstracts not directly exploring IoT adoption as a single technology were excluded. (e.g. Industry 4.0, IoT and Big data, IoT and Block chain, IoT and Artificial Intelligence, IoT and Machine learning) 3) Studies published before January 2020, were excluded.
Identifying Sources and Databases	We searched various digital databases (e.g. Scopus, Web of Science, IEEE Xplore, University of Botswana Library catalogue, and Google Scholar).

Stage	**Description**
Formulating Search Strategies	We used search terms and keywords like ("Internet of Things" OR IoT) AND (literature review OR systematic review) NOT Title ("Industry 4.0" OR "Block chain" OR "Artificial Intelligence" OR "Machine learning"). Additionally, we narrowed the focus of our search by combining ("Internet of Things" OR IoT) with the key terms like (history OR definition OR application OR technology OR architecture OR communication model OR standard OR protocol OR prediction OR benefit OR challenge)
Performing Classification Analysis	1) We utilised Zotero software to eliminate duplicate entries. 2) Two independent reviewers were engaged to screen the remaining studies based on the pre-defined selection criteria. 3) Any disagreements between reviewers were settled through a constructive discussion until a consensus was reached.

Figure 1 presents the PRISMA flow diagram that we followed for the SLR selection process for this study.

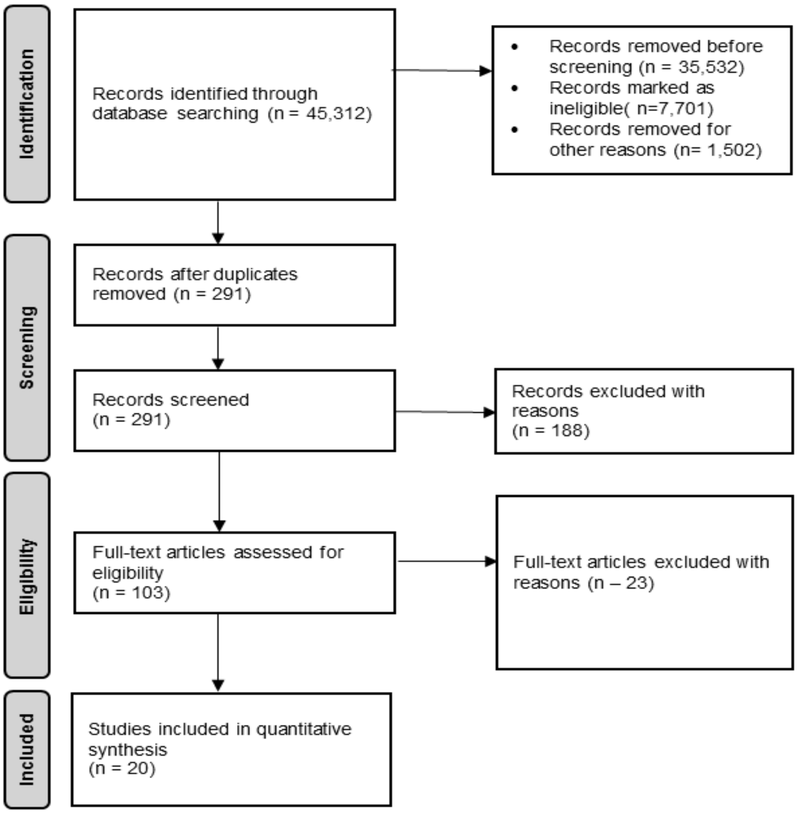
Identification
Records identified through database searching (n = 45,312)
Records removed before screening (n = 35,532)
Records marked as ineligible(n=7,701)
Records removed for other reasons (n= 1,502)
Screening
Records after duplicates removed (n = 291)
Records screened (n = 291)
Records excluded with reasons (n = 188)
Eligibility
Full-text articles assessed for eligibility (n = 103)
Full-text articles excluded with reasons (n – 23)
Included
Studies included in quantitative synthesis (n = 20)

Figure 1. PRISMA flow diagram followed by the study

Following the PRISMA protocol, we screened the titles and abstracts of the initial retrieved studies (45,312) using predefined inclusion and exclusion criteria (See Figure 1). Two independent reviewers evaluated these titles and abstracts to identify potentially relevant articles. Established criteria from resources like the Database of Abstracts of Reviews of Effects (DARE) and York University informed this process [17]. To ensure consistency, a standardised grading system with three options was employed: 'Yes' (scored 1), 'No' (scored 0), and 'Partially Meets Criteria' (scored 0.5). Reviewers documented their evaluations, and any discrepancies were resolved through discussion until consensus was reached. This rigorous screening process yielded 20 studies that comprehensively explore various topics related to the state-of-the-art IoT landscape. These studies were then selected for further analysis.

3. RESULTS AND DISCUSSION

This section presents the key findings from our SLR analysis on various topics in the IoT domain. These findings are discussed in detail in subsections 3.1 through 3.10.

3.1. IoT History

The “Internet of Things” (IoT) concept, though a recent buzzword, has roots in earlier inventions. While some trace it back to the 19th century's telephone [2], a more relevant starting point is the 1990s. This decade saw the emergence of the first internet-connected devices, like a toaster by John Romkey and a vending machine monitor at Carnegie Mellon [18]. Crucial advancements came in 1993 with Defense Advanced Research Projects Agency’s (DARPA) reliable satellite system, enabling Global Positioning System and paving the way for widespread internet access [19]. The coining of the term “IoT” is attributed to Kevin Ashton in 1999, who envisioned sensor-equipped objects communicating via the internet [20].

The 2000s witnessed a surge in wireless technology and “machine-to-machine” (M2M) solutions, fueling the explosion of connected devices. This era also saw the convergence of technologies like wireless networks, micro-sensors, and the internet, bridging the gap between operational and information technology [21]. The rise of smartphones and tablets further accelerated this growth [22]. Early examples of this trend include LG's introduction of the world's first internet-connected refrigerator in 2000. Soon after, in 2002, Sony and Philips collaborated to develop Near Field Communication Technology (NFC)[23]. By the mid-2000s, advancements in low-power sensors and cloud computing further propelled the IoT forward. Major organisations like Walmart adopted Radio Frequency Identification (RFID) for inventory tracking, demonstrating the practical applications of this technology [20],[24]. The rise of smartphones and tablets in the later part of the decade further accelerated this growth [22].

The 2010s witnessed the rise of the Industrial Internet of Things (IIoT) with industry giants like Cisco and IBM championing its adoption. Countries like China saw its strategic value, and pilot programs like "Smart City Switzerland" demonstrated its potential beyond consumer electronics [25]. These programs showcased how IoT could improve traffic management, energy efficiency, and other areas [25]. However, as IoT applications grew, relying solely on cloud computing for data processing became a bottleneck. Edge computing emerged as a solution, allowing data processing and analysis closer to the source. This reduced latency and improved real-time response times [26].

The later part of the decade (2017) saw the creation of a standardised vocabulary for IoT with the development of the “IoTOne” IoT terms database [27]. More recently, the 2020s have seen the powerful combination of Artificial Intelligence (AI) and Machine Learning (ML) with IoT technologies. This powerful combination unlocked new capabilities for data analysis, automation, and predictive decision-making in IoT applications [12]. Today, with billions of connected devices collecting and sharing data, IoT innovation thrives in healthcare, smart cities, and even the creation of digital twins, which are virtual replicas of physical systems [3].

3.2. IoT Defined

While the precise IoT definition is still under debate, it generally refers to the interconnection of physical devices embedded with sensors and software [3]. These “things” can exchange data and communicate with each other, creating a smart and interconnected environment [4]. There are many ways to understand IoT. Some understand it as a network of physical objects with unique identifiers, allowing them to communicate and collect data. Others envisage it as a vast system encompassing devices, machines, and even people, all interacting and sharing information [28]. At its core, IoT revolves around interconnected smart devices that exchange data over the internet. This data can be analysed to improve product development, service delivery, and maintenance processes. It essentially creates a world where objects can interact with their surroundings and each other to achieve specific goals [29]. The key aspects of IoT include smart devices, internet connectivity, data sharing, and interconnectedness. This technology allows for “any-time, any-place, anyone” connectivity, transforming the way we live and interact with the world around us [30].

Beyond data collection, IoT empowers remote control of connected devices, blurring the lines between the physical and digital worlds. It's a network that connects not just things, but also people, enabling them to share information and data like never before [31]. The most comprehensive definition considers IoT as a global infrastructure that integrates physical objects with the virtual world. These "things" become intelligent and capable of making decisions based on collected data [32]. This aligns with the growth of cloud computing and the expansion of the internet's addressing capacity [33]. In a nutshell, this broader understanding highlights the interdependence of everyday objects, individuals, and smart devices, all collaborating to foster a more intelligent and interconnected world [34]. Figure 2 depicts a schematic representation of the IoT system. This illustrates the interconnection of intelligent devices, facilitating communication and data exchange amongst them.

Figure 2. The IoT system [34]

3.3. IoT Enabling Technologies

The key technologies that enable IoT include Radio Frequency Identification, Near Field Communication, Wireless Sensor Networks, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, and LTE-A [5]. These technologies provide the specific networking capabilities required for an IoT system, which differs from a standardised network of conventional systems. In addition to these enabling technologies, IoT also relies on other technologies to fully leverage the opportunities it presents. These technologies embrace big data, cloud computing, sensors, and analytics software [35]. Below we provide a brief discussion of the key IoT enabling technologies [5], [35], [36].

1) **RFID:** It serves as a cornerstone technology within the IoT ecosystem. It facilitates seamless data exchange between everyday objects and a central hub, enabling real-time status updates without manual intervention. This technology pervades various industries, including retail, manufacturing, and logistics, by enhancing operational efficiency and connectivity through RFID-based IoT solution.

2) **Bluetooth Low Energy (BLE):** This technology focuses on short-range communication with low power consumption. It's ideal for applications like fitness trackers and real-time asset tracking due to its native support across many devices.
3) **NFC:** Similar to RFID, NFC offers a simple and energy-efficient way for devices to connect. The user-friendly "tap-and-go" approach makes it perfect for mobile payments and secure interactions between devices.
4) **Wireless Sensor Networks (WSNs):** Considered the sensory nervous system of IoT, WSNs collect data from the environment through sensors and transmit it to the internet. These networks are crucial for various applications like factory monitoring and environmental tracking.
5) **Cloud Computing:** Cloud services provide the infrastructure, platform, or software needed to run IoT applications. This allows firms to access resources and develops solutions without significant upfront investment.
6) **Big Data:** The massive amount of data generated by IoT devices necessitates tools for analysis and understanding. Big data analytics helps extract valuable insights from this vast information.
7) **Communication Protocols and Network Infrastructure:** Protocols act as the "traffic rules" for data transmission, ensuring smooth communication between devices. They define data formats and manage errors for reliable delivery. Cellular networks, Wi-Fi, and Long Range Wide Area Network (LoRaWAN) are some of the technologies that provide the "communication highways" for IoT devices.
8) **Embedded Systems:** These compact systems, combining hardware and software, are specifically designed for tasks within IoT devices. They collect, analyse, and transmit data, forming the core of many IoT solutions.

3.4. IoT Architectural Design

The IoT architecture serves as the underlying framework that enables communication between internet-connected devices. It encompasses multiple components, including layers, sensors, protocols, actuators, and cloud services [6], [8]. While there is no universally accepted design, researchers have proposed different architectures. Two main models are commonly discussed: the three-layered architecture and the five-layered architecture. The three-layered architecture comprises the application, network, and perception layers, representing the fundamental configuration. On the other hand, the five-layered architecture includes additional layers such as the business, application, processing, transport, and perception layers. These architectural models differ not only in functionality but also in the technical terminologies they employ [37]. To provide a visual representation of these layers, Figure 3 illustrates both the three-layered architecture (A) and the five-layered architecture (B).

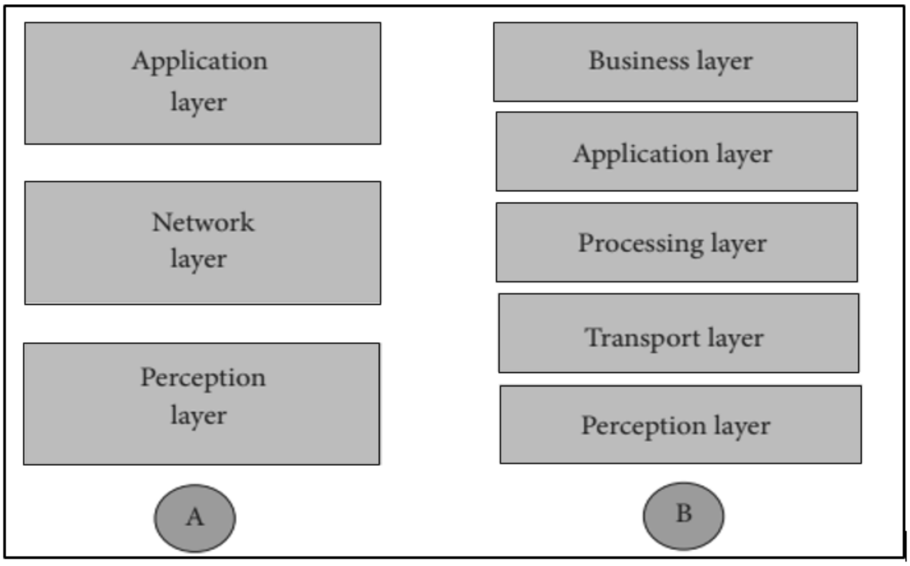

Figure 3. Architecture of IoT (A: three layered) (B: five layered)[37]

3.4.1. The three-layered architecture (Basic model):

1) **Perception Layer (Physical Layer):** This layer consists of the physical devices like sensors, cameras, and actuators that collect data from the environment and perform actions. They send this data to the next layer [37].
2) **Network Layer (Transmission Layer):** This layer manages communication between devices. It uses protocols like Wi-Fi, cellular networks, or Bluetooth to securely transmit data from sensors to the application layer [37].
3) **Application Layer:** This top layer processes the received data, analyses it, and presents it in a user-friendly way (like graphs or tables). It also allows users to control devices through apps or web interfaces [37].

3.4.2. The five layered architecture (More complex model):

This model adds two more layers for more sophisticated applications [37]:

1) **Transport Layer:** This layer sits between the perception layer and processing layer. It's responsible for efficiently moving data across networks (like Wi-Fi, local area network) from sensors to the processing layer.
2) **Processing Layer (Middleware Layer):** This layer acts like the brain of the system. It receives large amounts of data from the transport layer,

analyses it, stores it, and even performs tasks like big data processing. It often resides at the "edge" of the cloud for faster communication.

3.5. IoT Communication Models

There are four main communication models that dominate the IoT landscape. These communication models are briefly discussed as follows [8]:

1) **Request-response model:** This is a classic back-and-forth exchange. A device (like a sensor) sends a request for information to another device (like a server), which then responds with the data. Figure 4 illustrates the request-response model.

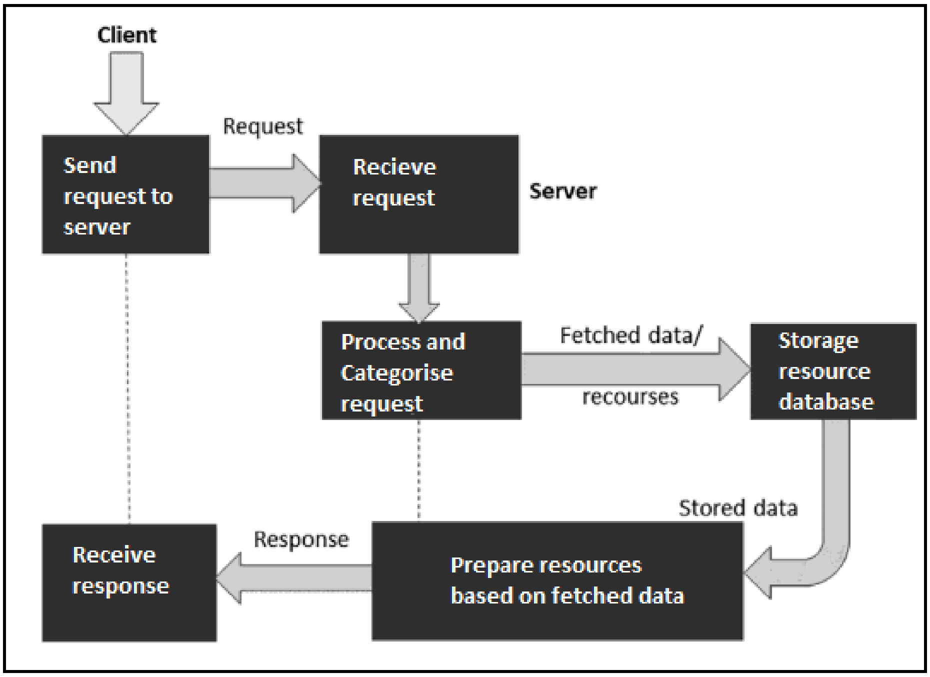

Figure 4. The request-response model [8]

2) **Publish-Subscribe model:** Unlike the Push-Pull model, devices in Publish-Subscribe (Figure 5) do not directly interact. Instead, publishers broadcast data to designated topics. "Subscribers" interested in that topic receive the data anonymously, eliminating the need for publisher identification.

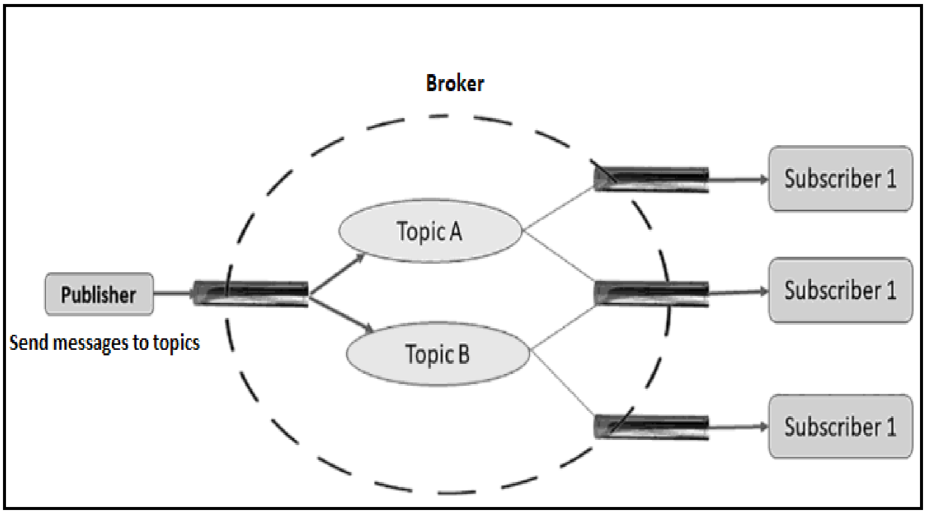

Figure 5. The publisher-subscriber model [8]

3) **Push-Pull model:** The Push-Pull model utilises a central data queue for communication (Figure 6). Devices can independently "push" data to the queue and "pull" required information at set intervals. This approach decouples data exchange, enabling smooth communication even with varying data rates between producers and consumers.

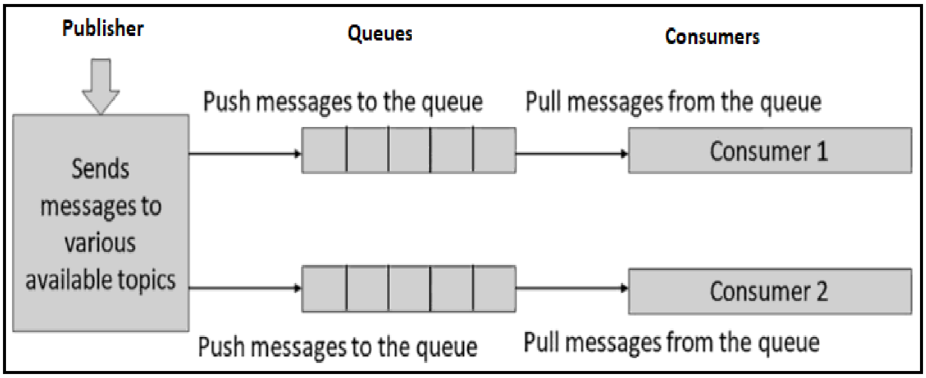
Publisher
Queues
Consumers
Sends messages to various available topics
Push messages to the queue
Pull messages from the queue
Consumer 1
Consumer 2
Push messages to the queue
Pull messages from the queue

Figure 6. The push-pull model [8]

4) **Exclusive-Pair model:** This is a direct, continuous connection between two devices. It's ideal for real-time, high-bandwidth communication. Figure 7 provides a visual representation of the Exclusive Pair model as shown.

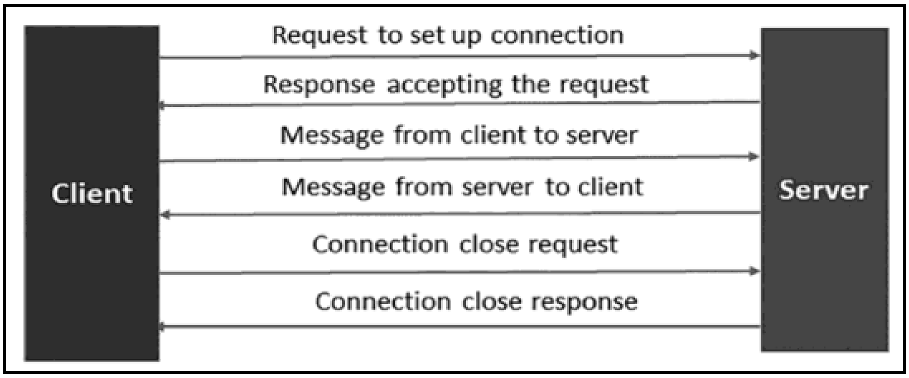
Client
Server
Request to set up connection
Response accepting the request
Message from client to server
Message from server to client
Connection close request
Connection close response

Figure 7. The exclusive-pair model [8]

3.6. IoT Standards and Protocols

The IoT relies on a well-defined set of communication guidelines known as protocols and standards. These protocols dictate how data is formatted and exchanged between devices, ensuring seamless communication within the network [38]. The development of these protocols is a collaborative effort driven by leading organisations like the Institute of Electrical and Electronics Engineers (IEEE), EPCglobal, the Internet Engineering Task Force (IETF), the European Telecommunications Standards Institute (ETSI), and the World Wide Web Consortium (W3C)[1]. Broadly, these protocols can be categorised into two main groups: data protocols (formatting information) and network protocols (device connection). These standards and protocols are discussed in detail in the subsequent sub sections:

3.6.1 IoT data protocols

A brief description of some key IoT data protocols is provided as follows [39]–[41] :

1) **Data Distribution Service (DDS):** DDS is known for its speed and real-time performance, making it suitable for high-volume data transmission. It is commonly used in applications like robotics and autonomous vehicles due to its low latency and reliable architecture.
2) **Hyper Text Transfer Protocol (HTTP):** HTTP is the foundation of web communication and is often used for heavy data transfers. While it is not ideal for battery-powered devices due to high energy consumption, industries like manufacturing rely on HTTP for its ability to handle large data loads.
3) **Advanced Message Queuing Protocol (AMQP):** AMQP excels in security and secure message exchange, making it popular in server

environments like banking. However, its resource-intensive nature limits its use with resource-constrained IoT devices.

4) **WebSocket:** WebSocket facilitates two-way communication over a single connection, making it suitable for scenarios with continuous data exchange. It finds applications in client-server environments.
5) **Constrained Application Protocol (CoAP):** CoAP is designed specifically for resource-constrained devices, offering a lightweight alternative to HTTP. It is ideal for devices with limited power and processing capabilities, such as smart energy and building automation applications.
6) **Extensible Messaging and Presence Protocol (XMPP):** XMPP is an open-source protocol widely used in messaging platforms. It provides flexibility and reliability for M2M communication, enabling secure exchange of structured and unstructured data formats.
7) **Message Queuing Telemetry Transport (MQTT):** MQTT is a lightweight protocol that uses publish-subscribe model for efficient data exchange. It minimises power consumption and is often used in industrial IoT. However, it lacks standardised data representation and device management, resulting in vendor-specific implementations.
8) **M2M Communication Protocol:** This open protocol enables affordable, two-way communication between internet-connected devices. It allows machines to self-monitor and adapt to changing environments, finding applications in smart homes, automated vehicles, and vending machines.

3.6.2 IoT network protocols

Below, we present a concise overview of key IoT network protocols [1], [42]:

1) **Bluetooth:** is a widely employed short-range wireless technology facilitating connectivity between devices such as smartphones and smart sensors with gateways. It's esteemed for its ease of use and minimal power consumption, particularly suitable for battery-operated devices.
2) **IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN):** is an open standard enabling low-power wireless technologies like BLE to access the internet. It's prevalent in applications like home automation and industrial monitoring.
3) **Zigbee:** serves as a low-power, low-data rate wireless network protocol often utilised in home automation and industrial environments. Known for its reliability, security, and support for various network topologies such as mesh networks, Zigbee scales well for numerous devices.
4) **Lightweight Machine-to-Machine (LwM2M):** is an industry protocol facilitating remote management of resource-limited devices and low-power sensors. It aids in cost reduction and expedites IoT solution development by enabling M2M communication over public networks, allowing devices to self-regulate in dynamic environments.

5) **NFC:** permits contactless data exchange within a short range, typically a few centimeters. Frequently used in mobile payments, identification documents, and key cards.
6) **LoRaWAN:** is an IoT protocol tailored for extensive networks housing millions of low-power devices. Offering long-range, low-power communication with robust signal penetration, LoRaWAN suits applications like smart cities requiring connectivity over expansive areas..
7) **Wi-Fi:** stands as a prevalent wireless technology facilitating high-speed data transmission across moderate distances. Though not optimal for all IoT devices due to its higher power consumption, Wi-Fi finds application in scenarios necessitating larger data transfers.
8) **Thread:** a newer networking protocol rooted in Zigbee, provides secure and efficient internet connectivity for devices in compact areas. Leveraging IPv6 for communication and boasting self-healing capabilities within the network, Thread often underpins the Matter protocol, fostering interoperability among diverse IoT devices.

3.7. IoT Applications

The pervasiveness of IoT lies in its diverse applications. From smart homes managing resources to wearables monitoring health, IoT is revolutionising industries. Industrial IoT streamlines production, predicts equipment failures, and optimises supply chains [49]. Agriculture benefits from real-time monitoring, leading to improved resource usage and crop yields [50]. The healthcare industry leverages IoT for remote patient monitoring and improved communication [51], while autonomous vehicles rely on it for safe navigation [52]. Figure 8 provides a comprehensive overview of a block diagram illustrating different application areas within the IoT.

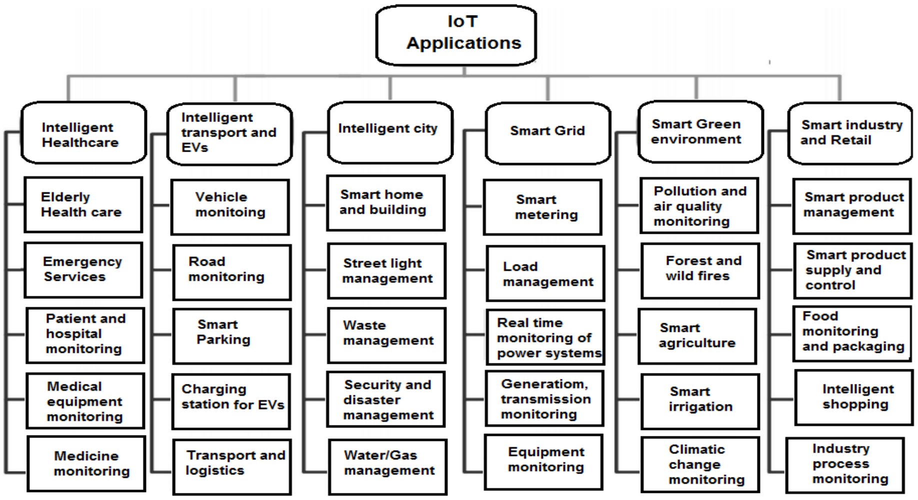

Figure 8. Block diagram of various IoT application domains [53].

3.8. IoT Predictions, Usage and Growth Statistics

The IoT is rapidly transforming the world, driven by a surge in connected devices and the promise of immense economic impact. Forecasts predict a staggering number of connected devices – exceeding 50 billion globally by 2025 [10] – translating to a multi-trillion-dollar market by 2030 [11]. This growth is particularly pronounced in the Asia-Pacific region, fueled by factors like remote operations, efficient supply chains, and expanding 5G networks [43]. Cost savings remain a key driver for IoT adoption, with over half of enterprises citing it as a major motivator [44]. Industrial applications account for a significant portion of projects, followed by transportation, energy, and healthcare. Notably, smart home devices are expected to remain dominant [11]. The widespread adoption is driven by the availability of cost-effective hardware like sensors and RFID tags [45].

Enterprise adoption of the IoT has witnessed a significant surge in recent years, with global spending projected to reach $1.1 trillion by 2023 [46]. The Asia-Pacific region has emerged as a leader in this growth, with a recent industry report highlighting it as the top spender on IoT in 2019. Notably, India contributed a significant amount, with spending reaching US$20.6 billion [46]. Some studies predict significant growth in the IoT device market, with estimates reaching $1.1 trillion by the end of 2026 [47]. Past industry forecasts anticipated a promising future for the global IoT market. Analysts predicted a Compound Annual Growth Rate (CAGR) of 21.9% from 2022 to 2023, translating to a market value reaching $486.7 billion in 2023, up from $399.41 billion in 2022 [48]. This surge in adoption underscores the growing recognition of the potential benefits that IoT offers for businesses across various sectors. Figure 9 depicts McKinsey Global Institute's estimations for the market share distribution of prominent IoT application areas. This illustrates that the healthcare industry was anticipated to hold the largest market share, followed by the manufacturing sector [27].

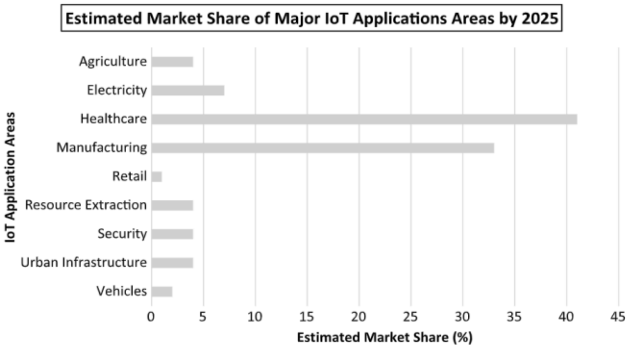

Figure 9. McKinsey Global Institute's 2025 projection of market share for key IoT application areas

3.9. IoT Adoption Benefits

The IoT is revolutionising businesses by boosting productivity, efficiency, and innovation. Experts predict companies that do not embrace IoT will fall behind competitors [54]. Table 2 provides a summary of IoT benefits as shown.

Table 2. An overview of IoT adoption benefits

Benefit	Description	Source
Enhanced productivity and efficiency	Automates tasks, gathers real-time data, optimises processes	[55]
Innovation	Enables new ways to interact with machines, fosters data-driven decision making.	[55]
Improved customer experience	Enables features like real-time tracking and personalised products.	[56]
Reduced costs	Minimises human error, optimises resource allocation, and predicts equipment failures.	[57]
Enhanced safety	Improves workplace safety through connected sensors and remote monitoring.	[58]
Stronger competitive advantage	Enables faster product development, data-driven marketing, and efficient operations.	[59]
Global market reach	Streamlines international operations and facilitates data exchange.	[59]
Stakeholder engagement	Creates a unified network for seamless collaboration.	[60]
Personalised Products and Services	Enables faster development of customised offerings.	[61]
Improved inventory management	Automates stock level monitoring and minimises manual intervention.	[55]
Customer-centric approach	Enables data-driven product development based on customer behaviour	[57]
Reduced operational costs	Automates workflows, minimises waste, and optimises energy usage	[62]
Streamlined supply chains	Enables real-time tracking of goods and optimises fleet management	[63]
Enhanced workplace safety	Monitors hazardous areas and processes, removes humans from potential danger.	[64]
Improved big data analytics	Integrates data for better decision making and forecasting	[65]
Enhanced customer convenience	Provides features like real-time delivery tracking and personalised notifications.	[57]

Source: Author

3.10. IoT Adoption Barriers

While the IoT offers significant benefits, realising its full potential can be challenging. Pansara [66] emphasises the importance of overcoming these challenges, as doing so can mitigate the fear of failure that often deters organisations from adopting IoT solutions despite their potential value [67]. Table 3 provides a summary of the key barriers organisations face when considering IoT adoption.

Table 3. An overview of IoT adoption barriers

Barrier	Description	Source
Security and privacy	Data breaches, unauthorised access, privacy concerns e.g. Anthem, Apple, Home Depot data breaches	[68]
Regulatory landscape	Lack of clear regulations, fragmented governance	[59]
Interoperability	Difficulty connecting devices and systems from different vendors.	[69]
Cost	High upfront and ongoing costs for hardware, software, and personnel	[70]
Lack of standards	Inconsistent standards hinder data sharing and integration	[71]
Business process integration	Difficulty adapting existing processes to work with IoT	[69]
Lack of awareness and skills	Employees unaware of IoT benefits, skills gap in management.	[72]
Vendor selection	Difficulty finding reliable vendors for scalable and secure solutions	[73]
Energy consumption	Large amounts of data require processing, increasing energy demand	[74]
Technical and business uncertainties	Evolving technology landscape, competition, future-proofing investments.	[75]
Limited internet infrastructure	Poor internet connectivity in some regions hinders scalability.	[76]
Unfulfilled expectations	Past technologies like RFID have not met initial hype.	[77]

Source: Author

4. CONCLUSION

This study investigates the IoT landscape through a systematic literature review methodology. This analyses publications from 2020-2024 alongside influential earlier works. The research explores the evolving landscape of IoT, encompassing its history, definitions, enabling technologies, architectures, communication protocols, applications, usage trends, and the potential benefits and challenges it presents. A key finding is the lack of a single, universally accepted definition for IoT. Similarly, architectural models vary across scholarly works, with three-layer models for basic applications and five-layer models for complex scenarios being most prevalent. Communication protocols are categorised into data and network categories. While IoT adoption offers immense potential, it also presents both advantages and disadvantages. The potential benefits include increased productivity, innovation, customer satisfaction, cost reduction, safety improvements, and a competitive edge for businesses. However, challenges persist in areas such as security, privacy, regulations, and interoperability. Concerns also remain regarding high costs, lack of standardisation, integration complexities, skill gaps, vendor selection, energy consumption, and unmet expectations. The study acknowledges the ongoing development of IoT and highlights the need for future research. This includes exploring the intricacies of the IoT protocol stack for secure communication possibly in digital twins, secure design architectures using blockchain. Moreover, future studies can explore seamless integration of IoT with AI and machine learning for intelligent automation.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Commun. Surv. tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] C. Ö. Sarışen, “A Study About the Influence of Purpose Limitation Principle Over the Function Creep in IoT Profiling,” TILT, Tilburg University, The Netherlands, 2023.

[3] S. Rangasamy, K. Rajamohan, V. S. Lavan, C. Mayur, and M. F. Lalitha, “Evolutionized Industry With the Internet of Things,” in *In Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries*, IGI Global, 2023, pp. 407–434.

[4] J. E. Ibarra-Esquer, F. F. González-Navarro, B. L. Flores-Rios, L. Burtseva, and M. A. Astorga-Vargas, “Tracking the evolution of the internet of things concept across different application domains,” *Sensors*, vol. 17, no. 6, p. 1379, 2017.

[5] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. H. C. D. Albuquerque, “MAC layer protocols for Internet of Things: A survey,” *Futur. Internet*, vol. 11, no. 1, p. 6, 2019.

[6] F. Firouzi, B. Farahani, M. Weinberger, G. DePace, and F. S. Aliee, *Iot fundamentals: Definitions, architectures, challenges, and promises*. 2020.

[7] geeksforgeeks, “Communication Models in IoT (Internet of Things),” *geeksforgeeks*, 2023.

[8] P. R. Gunjal, S. R. Jondhale, J. L. Mauri, and K. Agrawal, *Internet of Things: Theory to Practice*. CRC Press, 2024.

[9] H. H. Hasan and Z. T. Alisa, "Effective IoT congestion control algorithm," *Futur. Internet*, vol. 15, no. 4, p. 136, 2023.

[10] K. Elgazzar *et al.*, "Revisiting the internet of things: New trends, opportunities and grand challenges," *Front. Internet Things*, vol. 1, p. 1073780, 2022.

[11] F. Nizzi, T. Pecorella, F. Esposito, L. Pierucci, and R. Fantacci, "IoT Security via Address Shuffling: The Easy Way," *IEEE Internet Things J.*, vol. 6, pp. 3764–3774, 2019.

[12] H. Allioui and Y. Mourdi, "Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey," *Sensors*, vol. 23, no. 19, p. 8015, 2023.

[13] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions," *IEEE Commun. Surv. Tutorials*, 2023.

[14] M. Nassereddine and A. Khang, "Applications of Internet of Things (IoT) in smart cities," in *In Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy*, CRC Press, 2024, pp. 109–136.

[15] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement.," *PLoS Med*, 2009, doi: doi: 10.1371/journal.pmed.1000097.

[16] N. Shaheen *et al.*, "Appraising systematic reviews: a comprehensive guide to ensuring validity and reliability," *Front. Res. Metrics Anal.*, vol. 8, 2023.

[17] B. Farhan, "Theoretically assessed framework for cyberbullying prediction: a study on undergraduate students from universities in Malaysia using pls-sem and neural network approach," UTAR, 2023.

[18] J. S. Masip Capdevila, "Development of a gas monitoring system based on the internet of things," 2021.

[19] K. D. Foote, "A Brief History of the Internet of Things," *Dataversity*, 2022.

[20] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *In 2014 International Conference on Science Engineering and Management Research (ICSEMR)*, 2014, pp. 1–8.

[21] G. Aceto, V. Persico, and A. Pescapé, "A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3467–3501, 2019.

[22] M. A. Ezechina, K. K. Okwara, and C. A. U. Ugboaja, "The Internet of Things (Iot): a scalable approach to connecting everything," *Int. J. Eng. Sci.*, vol. 4, no. 1, pp. 9–12, 2015.

[23] A. Zrelli, "Hardware, software platforms, operating systems and routing

protocols for Internet of Things applications," *Wirel. Pers. Commun.*, vol. 122, no. 4, pp. 3889–3912, 2022.

[24] Z. Y. M. Yusoff, M. K. Ishak, and K. A. Alezabi, "The role of RFID in green IoT: A survey on technologies, challenges and a way forward," *Adv. Sci. Technol. Eng. Syst. J*, vol. 6, no. 1, pp. 17–35, 2021.

[25] R. Constantinescu and T. Edu, "Internet of Things (IoT) as an Instrument to Improve Business and Marketing Strategies. A Literature Review," *Eur. J. Interdiscip. Stud.*, vol. 14, no. 2, 2022.

[26] D. K. Saini and B. Y. Sandhiyaa, "IoT Ecosystem Implications to Real-World Security Scenario," in *In Cyber Defense Mechanisms*, CRC Press, 2020, pp. 75–83.

[27] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, p. e4946, 2020.

[28] A. S. Gillis, "What is internet of things (IoT)?," 2021.

[29] J. Fruhlinger, "What is IoT? The Internet of things explained," 2020.

[30] P. Jain, F. Adrangi, and M. Venkatachalam, "Cellular IoT Network Architecture," 623,942 B2, 2020.

[31] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in Internet of things," *CAAI Trans. Intell. Technol.*, vol. 3, no. 4, pp. 208–218, 2018.

[32] ITU, "New ITU standards define the internet of things and provide the blueprints for its development," *International Telecommunication Union*, 2012.

[33] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," *Comput. Sci. Rev.*, vol. 44, p. 100467, 2022.

[34] M. Humayun, "Role of emerging IoT big data and cloud computing for real time application," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, 2020.

[35] T. Kramp, R. Van Kranenburg, and S. Lange, "Introduction to the Internet of Things," in *Enabling things to talk: Designing IoT solutions with the IoT architectural reference model*, 2013, pp. 1–10.

[36] S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, "Internet of things (IoT) enabling technologies, requirements, and security challenges," in *In Advances in Data and Information Sciences: Proceedings of ICDIS 2019*, 2020, pp. 119–126.

[37] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, p. 9324035, 2017, doi: 10.1155/2017/9324035.

[38] V. P. Singh, M. N. Kumar, M. A. K. Misra, and P. Kuncha, *IoT Communication Protocols*. GCS PUBLISHERS, 2023.

[39] B. H. Çorak, F. Y. Okay, M. Guzel, S. Murt, and S. Özdemir, "Comparative Analysis of IoT Communication Protocols," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, 2018, pp. 1–6.

[40] D. Suleman, R. Shibl, and K. Ansari, "Investigation of Data Quality Assurance across IoT Protocol Stack for V2I Interactions," *Smart Cities*,

vol. 6, no. 5, pp. 2680–2705, 2023.

[41] K. B. A. Bakar, F. T. Zuhra, B. Isyaku, and S. B. Sulaiman, "A review on the immediate advancement of the Internet of Things in wireless telecommunications," *IEEE Access*, vol. 11, pp. 21020–21048, 2023.

[42] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, 2021.

[43] U. ESCAP, "Frontier ICTs for sustainable development for digital leaders: submodule C: Internet of Things.," 2022.

[44] R. Bašková, Z. Struková, and M. Kozlovská, "Construction cost saving through adoption of IoT applications in concrete works," in *In Proceedings of CEE 2019: Advances in Resource-saving Technologies and Materials in Civil and Environmental Engineering 18*, 2020, pp. 452–459.

[45] S. N. R. Kantareddy, I. Mathews, R. Bhattacharyya, I. M. Peters, T. Buonassisi, and S. E. Sarma, "Long Range Battery-Less PV-Powered RFID Tag Sensors," *IEEE Internet Things J.*, vol. 6, pp. 6989–6996, 2019.

[46] R. Patil, "The Future of Industrial Internet of Things (IIoT) after COVID19 Pandemic," *Int. J. Eng. Appl. Phys.*, vol. 1, no. 3, pp. 242–271, 2021.

[47] B. D. Huyghue, "Cybersecurity, internet of things, and risk management for businesses," Utica College, 2021.

[48] V. Gopinath, K. V. Rao, and S. K. Rao, "A comprehensive analysis of IoT security towards providing a cost-effective solution: a layered approach," *Int. J. Inf. Technol.*, vol. 15, no. 7, pp. 3813–3826, 2023.

[49] A. Tan, "IDC outlines growth drivers in industrial IoT in coming years," *FUTUREIOT*, 2023. https://futureiot.tech/idc-outlines-growth-drivers-in-industrial-iot-in-coming-years/ (accessed Nov. 09, 2023).

[50] S. Dhal *et al.*, "Internet of Things (IoT) in digital agriculture: An overview," *Agron. J.*, vol. 116, no. 3, pp. 1144–1163, 2024.

[51] W. Hua, "Impact of IoT Adoption and Application For Smart Healthcare," *J. Commer. Biotechnol.*, vol. 27, no. 4, 2022.

[52] C. Bautista and G. Mester, "Internet of things in self-driving cars environment," *Interdiscip. Descr. Complex Syst. INDECS*, vol. 21, no. 2, pp. 188–198, 2023.

[53] I. Rafiq, A. Mahmood, S. Razzaq, S. H. M. Jafri, and I. Aziz, "IoT applications and challenges in smart cities and services," *J. Eng.*, vol. 4, p. e12262, 2023.

[54] C. Arnold and K. I. Voigt, "Determinants of Industrial Internet of Things Adoption in German Manufacturing Companies," *Int. J. Innov. Technol. Manag*, vol. 16, p. 1950038, 2019.

[55] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, "Internet of Things research in supply chain management and logistics: A bibliometric analysis," *Internet of Things*, vol. 12, p. 100318, Dec. 2020, doi:

10.1016/J.IOT.2020.100318.

[56] I. C. Ehie and M. A. Chilton, "Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation 103166.," *Comput. Ind.*, vol. 115, 2020.

[57] S. Das, "The Early Bird Catches the Worm—First Mover Advantage through IoT Adoption for Indian Public Sector Retail Oil Outlets," *J. Glob. Inf. Technol. Manag.*, vol. 22, pp. 280–308, 2019.

[58] N. Mukati, N. Namdev, R. Dilip, N. Hemalatha, V. Dhiman, and B. Sahu, "Healthcare assistance to COVID-19 patient using internet of things (IoT) enabled technologies," *Mater. today Proc.*, vol. 80, pp. 3777–3781, 2023.

[59] S. D. Parab, A. Deshmukh, and H. Vasudevan, "Understanding the Drivers and Barriers in the Implementation of IoT in SMEs," pp. 267–279, 2023, doi: 10.1007/978-981-19-7971-2_26.

[60] S. Yadav, S. Luthra, and D. Garg, "Internet of things (IoT) based coordination system in Agri-food supply chain: development of an efficient framework using DEMATEL-ISM," *Oper Manag Res*, vol. 15, pp. 1–27, 2022, doi: 10.1007/s12063-020-00164-x.

[61] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," *Internet Things Cyber-Physical Syst.*, 2023.

[62] P. Onu and C. Mbohwa, "Industry 4.0 opportunities in manufacturing SMEs: Sustainability outlook," *Mater. Today Proc.*, vol. 44, pp. 1925–1930, Jan. 2021, doi: 10.1016/J.MATPR.2020.12.095.

[63] Y. Khan, M. B. M. Su'ud, M. M. Alam, S. F. Ahmad, A. Y. A. B. Ahmad (Ayassrah), and N. Khan, "Application of Internet of Things (IoT) in Sustainable Supply Chain Management," *Sustainability*, vol. 15, no. 1, p. 694, 2022, doi: 10.3390/su15010694.

[64] S. Bhatnagar, "A New Prototype Based Smart Health Monitoring System in IoT System," in *In 2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, 2023, pp. 1–7.

[65] K. Ahuja and A. Khosla, "Data analytics of IoT enabled smart energy meter in smart cities," *Cloud Comput. Geospatial Big Data Anal. Intell. Edge, Fog Mist Comput.*, pp. 155–175, 2019.

[66] R. R. Pansara, "IoT Integration for Master Data Management: Unleashing the Power of Connected Devices," *Int. Meridian J.*, vol. 4, no. 4, pp. 1–11, 2022.

[67] K. Shahzad, S. A. Khan, and A. Iqbal, "Factors influencing the adoption of Internet of Things (IoT) in university libraries: a systematic literature review (SLR)," *Electron. Libr.*, 2024.

[68] B. D. Weinberg, G. R. Milne, Y. G. Andonova, and F. M. Hajjat, "Internet of Things: Convenience vs. privacy and secrecy," *Bus. Horiz.*, vol. 58, no. 6, pp. 615–624, 2015.

[69] M. Ghobakhloo, M. Iranmanesh, M. Vilkas, A. Grybauskas, and A.

Amran, "Drivers and barriers of Industry 4.0 technology adoption among manufacturing SMEs: a systematic review and transformation roadmap," *J. Manuf. Technol. Manag.*, vol. 33, no. 6, pp. 1029–1058, Sep. 2022, doi: 10.1108/JMTM-12-2021-0505/FULL/PDF.

[70] Y. Mitake, Y. Tsutsui, S. Alfarihi, M. Sholihah, and Y. Shimomura, "A life cycle cost analysis method accelerating IoT implementation in SMEs," *Procedia CIRP*, vol. 104, pp. 1424–1429, Jan. 2021, doi: 10.1016/J.PROCIR.2021.11.240.

[71] M. C. Türkeş, I. Oncioiu, H. D. Aslam, D. I. Marin-Pantelescu, A. Topor, and S. Căpuşneanu, "Drivers and barriers in using industry 4.0: a perspective of SMEs in Romania," *Processes*, vol. 7, no. 3, p. 153, 2019.

[72] H. S. Birkel and E. Hartmann, "Impact of IoT challenges and risks for SCM," *Supply Chain Manag. An Int. J.*, vol. 24, no. 1, pp. 39–61, 2019.

[73] T. R. Wanasinghe, R. G. Gosine, L. A. James, G. K. I. Mann, O. D. Silva, and P. J. Warrian, "The Internet of Things in the Oil and Gas Industry: A Systematic Review," *IEEE Internet Things J.*, vol. 7, pp. 8654–8673, 2020.

[74] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future.," *J. Clean. Prod.*, vol. 274, p. 122877, 2020, doi: 10.1016/j.jclepro.2020.122877.

[75] D. Kiel, J. M. Müller, C. Arnold, and K. I. Voigt, "Sustainable industrial value creation: Benefits and challenges of industry 4.0," *Int. J. Innov. Manag.*, vol. 21, pp. 1–34, 2017.

[76] P. Okafor, *Benefits and Adoption of Internet of Things (IoT) to Nigeria's Small and Medium-Sized Enterprises (SMEs)*. 2023.

[77] R. Aggarwal and M. L. Das, "RFID security in the context of internet of things," *ACM Int. Conf. Proceeding Ser.*, pp. 51–56, 2012, doi: 10.1145/2490428.2490435.