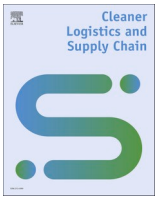
Cleaner Logistics and Supply Chain 4 (2022) 100065

Contents lists available at ScienceDirect

Cleaner Logistics and Supply Chain

journal homepage: www.journals.elsevier.com/cleaner-logistics-and-supply-chain



Internet of Things for sustainable railway transportation: Past, present, and future

Prashant Singh [a], Zeinab Elmi [a], Vamshi Krishna Meriga [a], Junayed Pasha [b], Maxim A. Dulebenets [a,*]

[a] Department of Civil & Environmental Engineering, Florida A&M University-Florida State University (FAMU-FSU) College of Engineering, 2035 E Paul Dirac Dr., Sliger Building, Suite 275, Tallahassee, FL 32310, USA
[b] Department of Biomedical, Industrial and Systems Engineering, Gannon University, 130 W 8th St, Erie, PA 16501, USA

ARTICLE INFO

Handling Editor: Shuaian Wang

Keywords:
Internet of Things
Rail transportation
Sustainable transportation
IoT benefits
IoT challenges
Railway applications

ABSTRACT

The Internet of Things (IoT) symbolizes numerous devices which are connected globally through the internet technology and are able to collect and share relevant data. The IoT has thus achieved a significant advancement in the field of sensors, networks, and communication technologies, such as long-term evolution (LTE) technology, fifth generation (5G) technology, wireless sensor networks (WSN), and others. Apart from technological advancements, the ability of IoT to run fully embedded (with or without an operating system), gather real-time data, estimate physical parameters, facilitate decision making based on the data gathered, use of various networks (e.g., local area networks (LAN), low-power wide-area network (LPWAN), cellular LPWAN) has provided enormous opportunities for its applications in the railway industry and other domains. The current study performs a comprehensive holistic survey of various IoT technologies that can be used in railway operations, management, maintenance, video surveillance, and safety at level crossings. This study also discusses current trends in the IoT, emerging IoT technologies, green IoT applications, and various research studies that have been conducted in the areas related to railway applications. Furthermore, various challenges that are associated with the IoT applications are discussed along with potential efforts that can be made to overcome these challenges. The outcomes of this work are expected to offer important insights regarding the applicability of IoT technologies for sustainable railway transportation, their future potential, operational benefits to relevant stakeholders and authorities, as well as critical future research needs that have to be addressed in the following years.

1. Background

The Internet of Things (IoT), which is also known as the Internet of Objects, is expected to change the world beyond imagination. The internet has a profound impact not only on daily lives of human beings but also on various domains, including education, business, transportation, infrastructure, smart cities, commercial, healthcare, and government. In recent decades, the internet has become a very powerful tool which has helped improving living standards and provided several types of safety measures with the integration of various technologies. The IoT is viewed as an emerging technology which uses the internet to identify the objects by themselves and attain intelligent behavior in a way that they can communicate the information about themselves with other connected devices (Zeinab and Elmustafa, 2017). Based on the IoT concept, anything (device or applications) can communicate with the internet at any time at any place to provide the information or services to anyone by any network (Fig. 1).

The concept of IoT to be used in the industry was first realized by the use of Radio Frequency Identification System (RFID) tags embedded in objects, the idea of which was proposed by Charles Walton in 1983 (Paragon, 2021). The European Union first adopted the concept of IoT in March 2007 by the commission of communication on RFID followed by the United States (U.S.) in 2008 (Sundmaeker et al., 2010). China and Japan officially adopted the IoT concept around the same time. As a part of the 7th research framework program on the information and communication technology theme, many different European companies belonging to the IoT community (e.g., SAP AG, Fraunhofer, Thales, ATOS, Ericsson, TXT, GS1, Alcatel, Telefonica, and Sapienza) submitted

* Corresponding author.
E-mail addresses: prashant1.singh@famu.edu (P. Singh), ze20a@fsu.edu (Z. Elmi), vm21l@fsu.edu (V. Krishna Meriga), junayed729@gmail.com (J. Pasha), mdulebenets@eng.famu.fsu.edu (M.A. Dulebenets).

https://doi.org/10.1016/j.clscn.2022.100065
Received 20 June 2022; Accepted 21 June 2022
Available online 25 June 2022

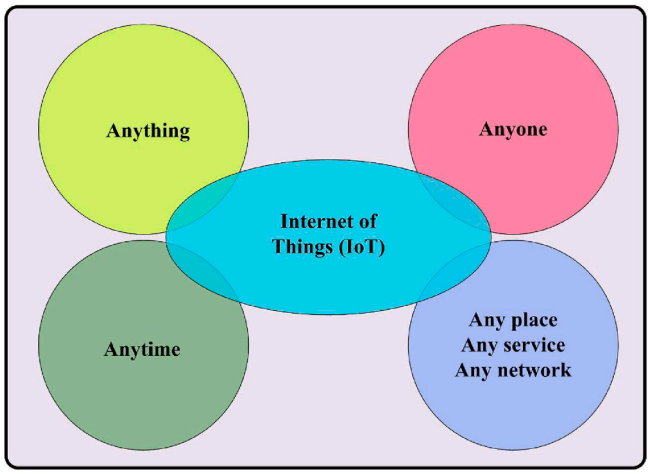


Fig. 1. Concept of Internet of Things (IoT).

collaborative proposals for the IoT improvements in 2009. The growth of IoT technology has been manifold in recent decades, and the number of connected devices is likely to increase exponentially with the growth of new technologies in the coming years (Sundmaeker et al., 2010). Fig. 2 illustrates the number of IoT-connected devices between 2019 and 2030. It is projected that the number of IoT-connected devices will grow by approximately 2.5 times between 2021 and 2030. Such a pattern can be explained by a rapidly changing technology globally and demand for the IoT-based technologies (Statista.com, 2021).

The IoT applications are rapidly growing in different domains across the globe and expanding in different areas, such as transportation and logistics, healthcare, manufacturing, agriculture, personal and social areas (Li et al., 2015; Jo et al., 2017; Jamkhaneh et al., 2022; Seuring et al., 2022). Fig. 3 shows the IoT infrastructure expenses by different verticals of industry for the years of 2015 and 2020. It can be observed that all the verticals have seen a tremendous spending in the IoT technology between 2015 and 2020. However, certain verticals, such as discrete manufacturing, transportation and logistics, and utilities, show the highest spending in the IoT technologies and its applications, followed by business-to-consumer (B2C), healthcare, and process domains. Moreover, the IoT concept has helped developing a variety of applications that have been used in smart cities to improve automation, energy saving, safety and security alerts, communications, and entertainment (Saranya and Nitha, 2015; Kaur and Singh, 2016). The growth of IoT applications is expected to be much faster than before due to the emergence of new communication technologies, such as the sixth generation (6G) technology, seventh generation (7G) technology, and federated learning (FL) that combines wireless communications with machine learning which have the potential to run the IoT applications in a safer, faster, and more reliable way beyond imagination (Liu et al., 2020; Yang et al., 2021).

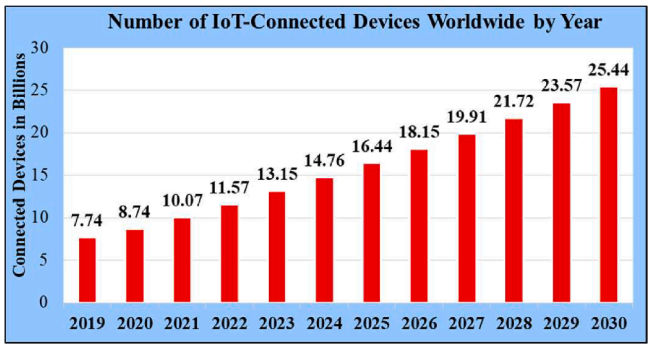


Fig. 2. Number of IoT-connected devices between 2019 and 2030.

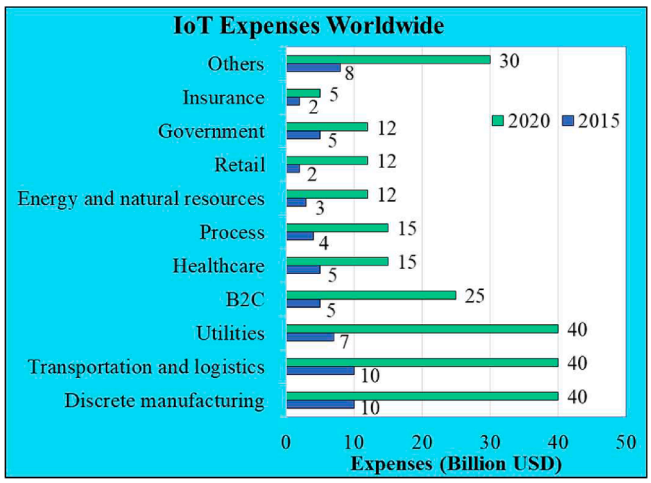


Fig. 3. Worldwide spending on the IoT by verticals (billion USD) for 2015 and 2020.

The IoT technology has been heavily used in railway applications, including railway operations, management, maintenance, video surveillance systems, and train control systems (Singh et al., 2021a). The IoT devices provide uninterrupted connectivity using the next generation internet and wireless communication with various applications deployed by autonomous trains. With the development of certain technologies, such as advanced computing, fog computing, artificial intelligence (AI), big data analytics, and machine learning (ML), large quantities of data can be processed using the IoT which helps improving efficiency and safety of the overall autonomous train system. The future growth in connected devices (see Fig. 2) will see huge potential for the IoT applications in the railway industry (especially for autonomous trains) and other domains as well (Kimiagar, 2019; Bogaard, 2020; Lambert, 2020). The use of futuristic technologies in the IoT applications is likely to help significantly reducing crashes at highway-rail grade crossings (or level crossings), where there is always a risk of potential conflicts between vehicles and trains at the same elevation (Singh et al., 2021a).

Several studies have been conducted to date and discussed the use of IoT technology, IoT challenges, opportunities, future research needs, and emerging technologies for the IoT (Sundmaeker et al., 2010; Zhao and Ge, 2013; Bansal and Lal, 2019; Chen, 2020; Stoyanova et al., 2020). However, no significant efforts have been made towards developing a detailed understanding of the IoT applications specifically in the railway industry, associated challenges, and critical future research needs. Therefore, this study aims to conduct a comprehensive and holistic review of the state-of-the-practice and the state-of-the-art to identify the existing IoT technologies, applications of various IoT technologies, current trends in the deployment of IoT technologies for railway-specific needs along with the associated next generation technologies, main challenges, and opportunities for the future research. The next sections of the manuscript are organized as follows. The second section aims to develop an understanding for the IoT-based technologies. A detailed review of the relevant state-of-the-art efforts dealing with the IoT applications is presented in the third section. The fourth section presents the state-of-the-art summary and identifies the main advantages of the IoT technologies in rail transportation along with the associated challenges. The study conclusions and potential future research needs are further presented in the fifth section. The list of abbreviations that are used within this manuscript is provided in **Appendix**.

2. Understanding the IoT technology

The IoT is considered as an addition to the current applications by introducing a new aspect of “Things” communication and integration.

The IoT will provide a value addition to the existing identification and data capturing capabilities as well as other associated cutting-edge technologies. The IoT technologies are classified as follows: (1) identification technologies; (2) IoT architecture technologies; (3) communication technologies; (4) network technologies; (5) network discoveries; (6) software-related algorithms; (7) hardware-related technologies; (8) signal and data processing technologies; (9) search and discovery engine technologies; (10) network management-related technologies; (11) energy storage and power technologies; (12) privacy and security technologies; and (13) standardization (Sundmaeker et al., 2010). Fig. 4 shows the important elements of the IoT which include the IoT nodes, fog nodes, cloud nodes, platforms, and applications. This section of the manuscript focuses on a detailed review of the key IoT technologies, major IoT applications, and current IoT trends in the railway industry.

2.1. Key IoT technologies

The IoT-based technologies can be classified into two major groups based on their applications (Sundmaeker et al., 2010): (1) enabling building block technologies that play a direct role in the IoT development; and (2) synergistic technologies that provide an added value to the IoT. Enabling building block technologies include electronic communication protocols, machine-to-machine interfaces, microcontrollers, RFID technologies, wireless communication, sensors, location technologies, actuators, and software. One the other hand, synergistic technologies are represented by geo-tagging/geo-caching, machine vision, biometrics, robotics, mirror worlds, augmented reality, adjustable autonomy, life recorders, tangible user interfaces, personal black boxes, and clean technologies. Some of the key IoT technologies will be further discussed in the following sections of the manuscript, including fog computing, RFID technology, wireless sensor networks (WSN), cloud computing, 5G technology, and big data analytics. Understanding the key IoT technologies would be essential before discussing the IoT applications in the railway industry.

2.1.1. Fog computing

Fog computing is an IoT concept that incorporates services, such as computing, storing, and networking, in a scattered fashion among end devices and classical cloud computing. Fig. 5 illustrates an overview of fog computing which includes a certificate authority (CA), a back-end cloud, fog nodes, and IoT devices (Alrawais et al., 2017). Fog computing offers the best solutions to the latency-sensitive IoT applications (Verma et al., 2016, Atlam et al., 2018). The fog computing technology was developed to fill in the existing gaps between the IoT devices and data centers. Some of the major advantages of fog computing technology are improved security, reduced bandwidth, and decrease in latency. Various applications of fog computing in the IoT include: (1) connected vehicles; (2) smart traffic lights; (3) smart homes; (4) wireless sensors and actuator networks; (5) healthcare and activity tracking; (6) IoT and cyber physical systems; and (7) augmented reality (AR).

Although fog computing is an important extension of cloud computing, certain issues related to privacy and security of network will continue to exist (Alrawais et al., 2017). The privacy and security issues can be caused by a lack of memory and computational power to execute certain cryptographic operations that are essential for proper

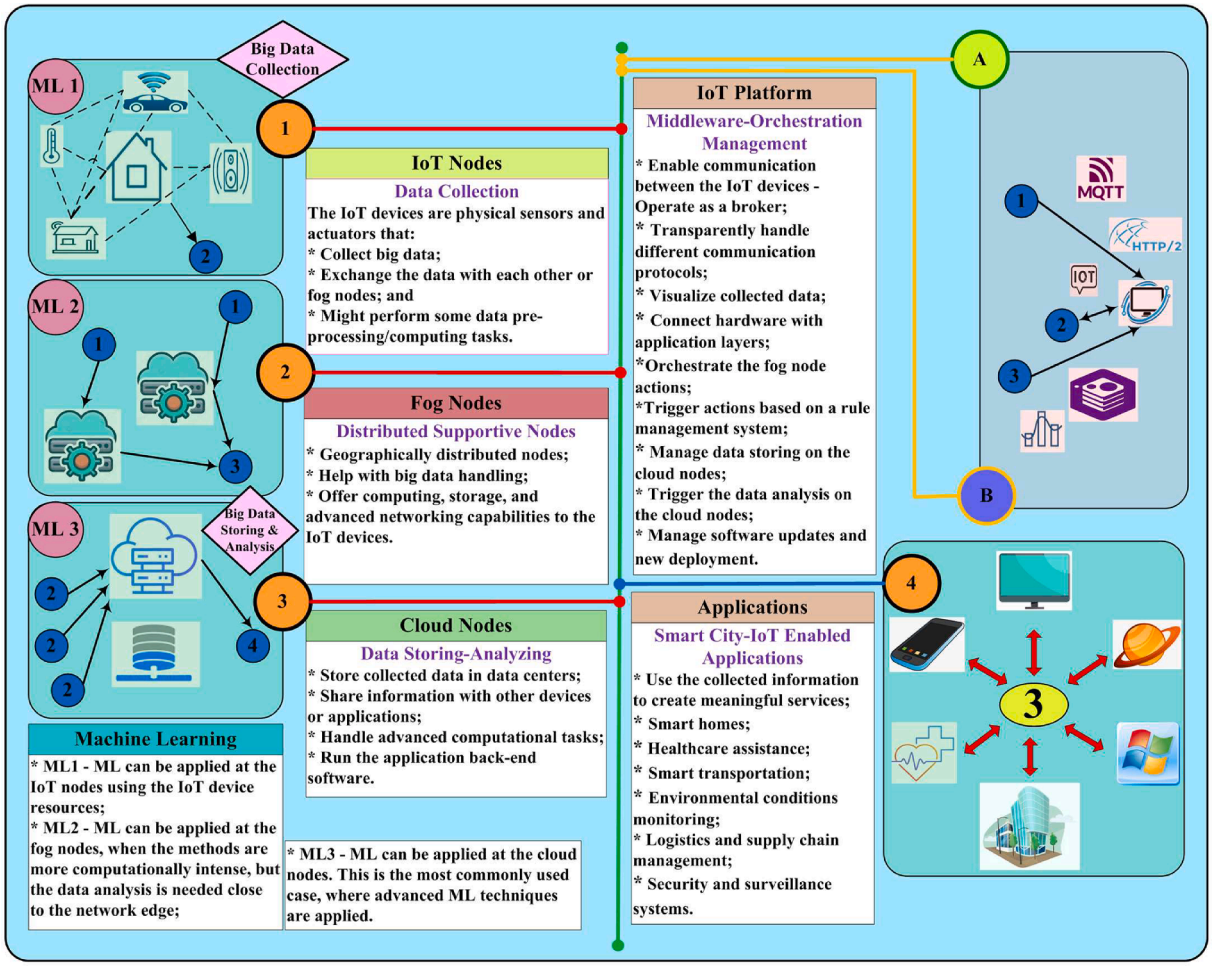


Fig. 4. Key elements of the IoT.

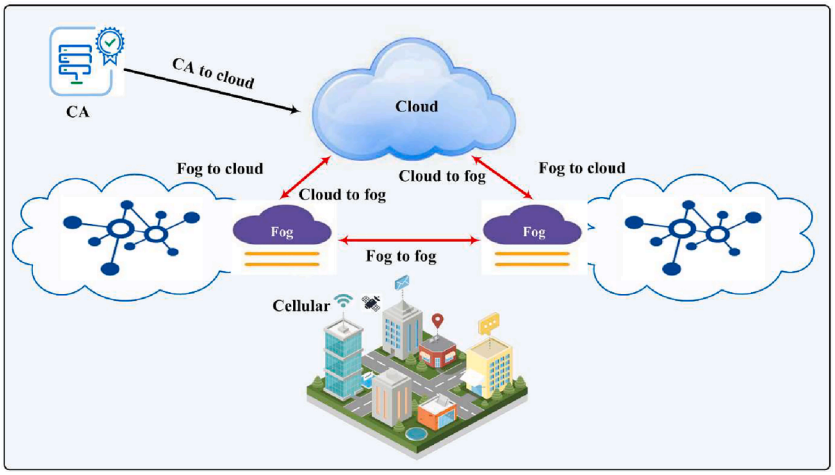


Fig. 5. Fog computing in the IoT network.

authentication, trust to the IoT devices, identification of rogue IoT nodes, access control, data aggregation, and other functions. Along with privacy and security, there are some other issues associated with fog computing that include scalability, complexity, dynamic nature, heterogeneity, management of resources, and consumption of energy (Luan et al., 2015; Yi et al., 2015; Choi et al., 2017; Mukherjee et al., 2017; Ni et al., 2017; Atlam et al., 2018).

2.1.2. *RFID technology*

The Radio Frequency Identification System (RFID) is a technology that works in an autonomous mode and assists machines or computers to detect objects, perform data recording, and uses radio waves to control independent targets. Once RFID tags are attached to the objects, an RFID reader which is connected to the internet can detect, monitor, and track any object automatically in real time globally. The ability of RFID using the internet makes it a major component of the IoT (Deng, 2012; Jia et al., 2012). The RFID technology has numerous and extensive applications. Some of the important applications are in process control during production, supply chain management, and object tracking management. Furthermore, a few of the broader areas of RFID applications are: (1) transportation and logistics; (2) manufacturing; (3) agriculture management; (4) medicine and healthcare industry; (5) operations of freight terminals; (6) defense and military; (7) financial transactions; (8) environmental monitoring and disaster early warning; and (9) warehouse and distribution.

Additionally, RFID readers can be used in combination with smartphones to easily authenticate and manage the objects (Park, 2018). For example, the High Frequency (HF) RFID technology has been used by the universities in China for student identification devices. Moreover, the Wireless Radio Frequency (WiRF) system can record student behavior and maintain automatic attendance records (Tan et al., 2018). The RFID technology has also been successfully used in the children's safety program for tracking and monitoring children from their home to school and vice-versa. The RFID technology can monitor and track children who are boarding and deboarding a bus (D'Errico et al., 2017). Chipless RFID continues gaining its popularity in different domains, especially in remote sensing applications (Mc Gee et al., 2019). Fig. 6 shows the main components of the RFID system that enable a flow of the data between tags and readers to be further used in the designated applications.

2.1.3. *Wireless sensor networks*

The wireless sensor networks (WSN) technology functions as a system of different nodes that work in synchronization with each other to sense and control the environment in their vicinity. This network of nodes that are linked to each other using wireless connection enables the

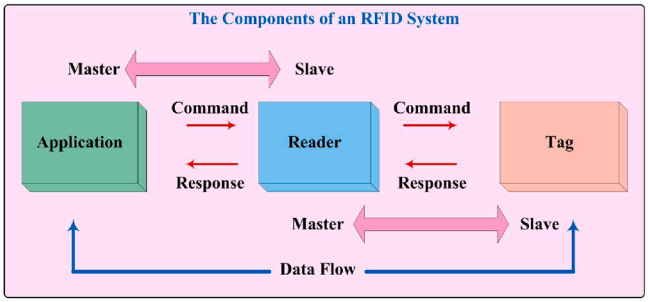


Fig. 6. The main components of an RFID system in the IoT framework.

nodes to communicate with each other. There are three major elements of the WSN architecture: (1) sensor nodes; (2) gateway; and (3) users (observers) (Ephrem, 2015; Kocakulak and Butun, 2017). The key function of the sensing unit is to sense the environmental conditions, such as temperature, pressure, heat, and humidity. The main computations are performed by the CPU once the sensing and monitoring process is completed by the sensor nodes. At the end, radio units transmit the computed data to the gateway by means of wireless connection. The users can further access the data via the internet. The main components of the WSN system are shown in Fig. 7. Zigbee, Z-wave, INSTEON, and WAVENIS are some examples of technologies used by the WSN (Kortuem et al., 2009; Mainetti et al., 2011). A number of WSN implementation challenges have been identified over the years (Alcaraz et al., 2010; Li and Kara, 2017): (1) large quantity of data; (2) network robustness; (3) consumption of power; (4) high cost; and (5) security of data. The WSN have been used in a variety of applications, including infrastructure

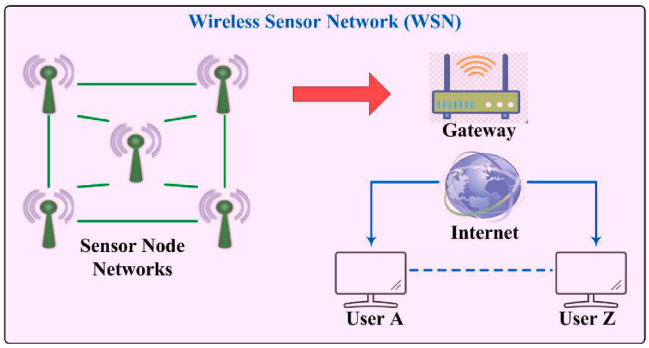


Fig. 7. The main components of the WSN system.

monitoring, supervising, and monitoring of medical equipment in healthcare settings (Armentia et al., 2015; Aono et al., 2016; Cabra et al., 2017). Furthermore, the WSN in combination with IoT, big data, and 5G play a major role in disaster management (Adeel et al., 2019).

2.1.4. Cloud computing

Cloud computing is related to applications that are rendered as services over the internet along with hardware and software in the data storing centers that render these services (Armbrust et al., 2010). Cloud computing aims to satisfy rigorous standards which focus on providing customized, reliable, and quality of service (QoS)-oriented dynamic computing conditions for end users (Wang et al., 2010; Tyagi and Kumar, 2020). The architecture of cloud computing contains two parts (front end and back end) that are interconnected through the internet network. The key layers and services of cloud computing encompass a cloud client, a cloud application, platform services, infrastructure services, and a server (Jadeja and Modi, 2012). Cloud computing can be deployed in different ways (i.e., public cloud, private cloud, and hybrid cloud). A public cloud enables users accessing the cloud via web-browsers at a particular cost. Each private cloud is specific to a certain organization. On the other hand, a hybrid cloud represents a combination of public and private clouds.

The cloud computing technology has several advantages when it is integrated within the IoT framework. Some of the major advantages are (Jadeja and Modi, 2012): (1) simple to manage; (2) decrease in cost; (3) availability of steady service; (4) disaster management applications; and (5) green computing where substantial emissions due to excessive use of systems can be reduced. Similar to other IoT-based technologies, cloud computing also faces various challenges, such as security, privacy, and reliability. Other identified challenges are associated with cloud adoption issues (e.g., cost of the cloud model, charging model, service-level agreements, types of data to migrate) (Dillon et al., 2010). Recent studies on cloud computing have focused on deep learning architectures in the cloud computing technologies. It is expected that various challenges encountered due to upcoming cloud computing architectures can be solved by different deep learning algorithms due to their ability to effectively analyze large quantities of data (Jauro et al., 2020).

2.1.5. 5G technology

The 5G is also known as the fifth generation communication technology that employs a millimeter wave (mmWave) technology as the main component apart from other components, such as (Sayrafian and Yazdandoost, 2015): (1) multiple-input-multiple-output (MIMO); (2) cloud-based network; (3) cognitive radio (CR) technology; and (4) device-to-device (D2D) communications. Fig. 8 shows the basic architecture of the 5G technology and its main components. It can be observed that the 5G terminal directly interacts with data servers, real-time communication servers, and control system policy servers via different communication technologies, including general packet radio services (GPRS), external devices (ED), gigabit ethernet (GE), the third generation (3G) technology, wireless local-area network (WLAN), and long-term evolution (LTE) technology (Li et al., 2018; Verma and Verma, 2021). The 5G model relies on the Internet Protocol (IP). The 5G architecture includes user terminals that have autonomous radio technologies. These radio technologies are further used as an IP connection to the internet world. The blockchain, encryption, and network-slicing are also directly used by the 5G (Ji et al., 2018; Chu et al., 2020). The software defined networking (SDN) is generally incorporated within the 5G technology to lower the cost of operation and equipment, whereas the network function virtualization (NFV) is used for intelligent manufacturing concepts (Rendon et al., 2019; Awoyemi et al., 2020).

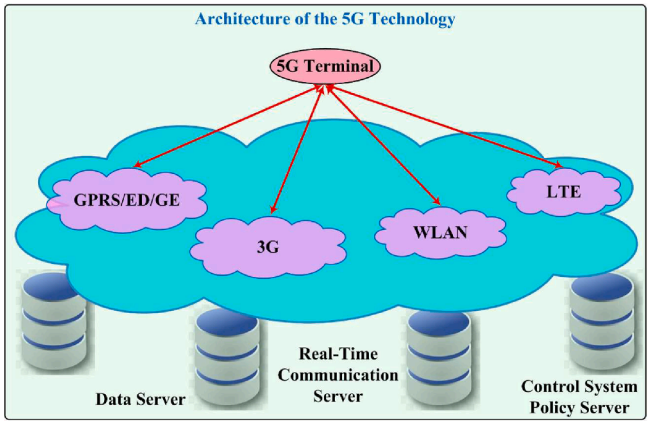


Fig. 8. The architecture and main components of the 5G technology.

There are various challenges in the deployment of 5G technologies that include, but are not limited to, the following (Verma and Verma, 2021): (1) the 5G technology significantly differs from the 4G technology (i.e., it has different type of macro-cells) which may create interference issues; (2) dense access points used by the 5G technologies can result in high latency and low throughout; (3) interaction between hundreds of different devices can be challenging; (4) governmental regulations and cybersecurity requirements of certain countries may impose additional challenges in the 5G implementation; (5) maintenance requirements and infrastructure development; (6) privacy and security; (7) social and environmental impacts of the 5G technologies; and (8) standardization of the 5G services.

2.1.6. Big data analytics

Big data analytics is one of the most significant phenomena in the business intelligence (BI) combining the two: big data and analytics (Russom, 2011). There are several data processing and analytical platforms which are used for analyzing an enormous amount of the generated IoT data. Some of the available platforms are (Ahmed et al., 2017): (1) Apache Hadoop; (2) 1010data; (3) Cloudera data hub; (4) SAP-Hana; (5) HP-HAVEn; (5) Hortonworks; (6) Pivotal big data suite; (7) Infobright; and (8) MapR. The main requirements of big data analytics are connectivity, storage, quality of service, real-time analytics, and benchmarks. The IoT applications generate a large amount of information and are the main source of big data. Some of the major advantages of big data applications in the IoT are (Bessis and Dobre, 2014; Al Nuaimi et al., 2015; Hashem et al., 2016): (1) smart transportation – lowering the number of crashes, minimize congestion of traffic, optimization of vehicle movements, and highway safety; (2) smart healthcare – help in developing better insurance policies, detection of early warning signs of any serious disease, forecasting cure, epidemics and diseases; (3) smart grid – develop optimal pricing plans based on the consumption of power, forecasting future needs, ensuring sufficient amount of power supply; and (4) smart inventory system – detection of fraud cases, understanding needs of customers, and recognize probable risks. Fig. 9 shows a general process of big data flow in the IoT which directly involves data collection, storage, monitoring, and analytics.

2.2. Major IoT applications

2.2.1. Blockchain

The blockchain is a shared and unchangeable record that assists in the process of registering various transactions and facilitates management of different assets (both tangible, such as a car, cash, house, land etc., and intangible, such as patents, copyrights, branding, etc.) and tracking them within a business network. Typically, any commodity having a value can be peddled and tracked within a blockchain network which further lowers the cost and risk for all (IBM, 2021). The main characteristics of the blockchain technology are (Atlam and Willis, 2019): (1) decentralization; (2) immutability; (3) transparency; (4) better security; and (5) efficiency. The blockchain can improve the IoT by providing secure service and accessibility to authentic data (Karthikeyyan and Velliangiri, 2019).

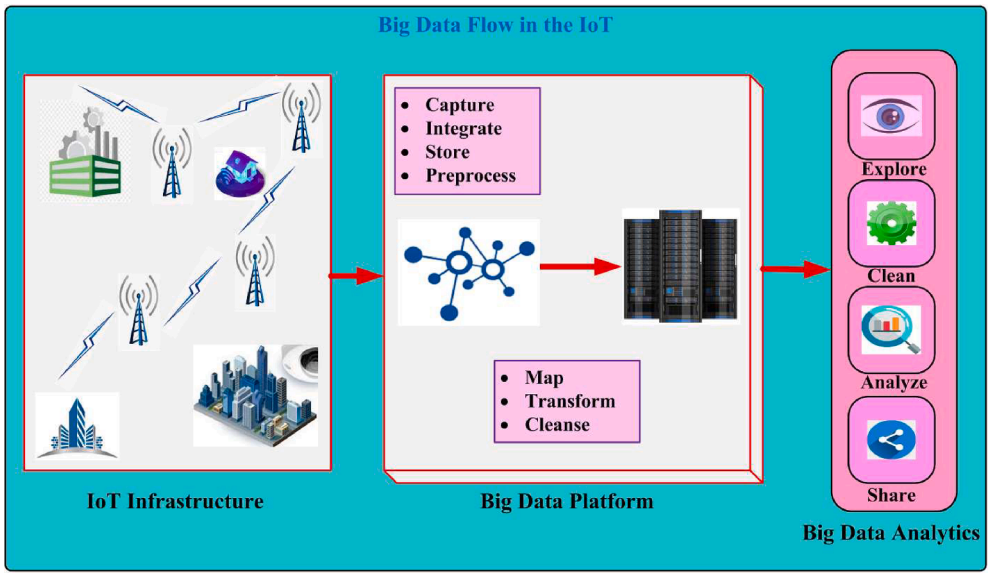


Fig. 9. Big data flow in the IoT.

However, the blockchain and IoT technologies have some distinct differences in terms of certain attributes, such as amount of required resources, complexity of processes, system restrictions, and bandwidth characteristics (Kumar and Mallick, 2018; Xu et al., 2018) – see Table 1. There are many different areas of blockchain applications in healthcare, energy, voting systems, stock exchange, insurance management, cybersecurity, asset tracking, digital records, law enforcement, identity management, education, and other domains (Nofer et al., 2017; Naser, 2018; Monrat et al., 2019). However, there are a lot of barriers and challenges associated with successful applications of the blockchain technology. These challenges include, but are not limited to, scalability and performance, privacy issues, interoperability, energy consumption, fairness and security, and existing regulation-related issues (Monrat et al., 2019).

2.2.2. *Transportation domain*

The IoT applications have shown significant capabilities to alter the transportation industry by transforming the way information and data are being collected and ensuring an effective transfer of the important technical and business data, analytics, mobility, and automation (AL Enterprise, 2020). With the expansion of IoT technology in transportation, transportation systems nowadays can "feel" and "think" which further contributes to the development of Intelligent Transportation Systems (ITS). By using vehicle-installed sensors and mobile devices, transportation systems can optimize route selection, offer parking spot reservations, provide smart lighting, enable crash mitigation, smart public transportation, as well as connected and autonomous driving (Zantalis et al., 2019). The IoT technologies are heavily used in smart traffic lights and supervision of green time monitoring at intersections via cloud management. Also, traffic prediction can be accomplished by using the archival data with smart IoT technologies. The IoT applications mitigate congestion in smart cities (Perwej et al., 2019), which further reduces the amount of emissions produced by vehicles and promotes sustainable transportation. Smart ITS are being developed to address real-time issues involving tracking vehicle location, intelligent parking systems for vehicles, big data mining for transportation systems, and communications (Muthuramalingam et al., 2019). The deployment of real-time optimization approaches that directly rely on big data and IoT has the potential of improving the performance of transportation systems, including railway systems as well.

As an example, the Aircraft Monitoring and Electronically Linked Instantaneous Analytics (AMELIA) is one of the successful IoT-based applications that have been intensively used in the airline industry. The AMELIA relies on edge computing and can detect any exigency in the aircraft operations (Pate and Adegbija, 2018). The system can transmit necessary data and information that can be further used to facilitate emergency response. Fig. 10 depicts the AMELIA's architecture. The AMELIA application receives the data from the on-board flight data acquisition unit (FDAU). Most of the aircrafts with the state-of-the-art technology have an onboard FDAU with numerous interfaces and input ports that enable flight data recording. The AMELIA has different layers that keep the record of emergency alerts based on the obtained flight data and provides ranking of emergency alerts which is essential for proper response.

Various IoT-based applications have been used in the shipping industry as well, including but not limited to the following: (a) cloud computing (based on user needs, configuration and provision of resources can be arranged); (b) message queuing telemetry transport (MQTT) protocol which is primarily used for machine-to-machine communications; and (c) docker images which are an open-source technology that permits users to create, develop, and run container-related applications in an autonomous mode. The IoT-enabled containers allow continuous supervision of the information related to humidity, temperature, luminosity, and vibrations throughout the entire transportation process (Salah et al., 2020). Fig. 11 illustrates the system architecture of smart containers being used in the shipping industry. It can be observed that the IoT-enabled containers have a variety of sensors that can accurately monitor the cargo status. The collected cargo data can be directly transmitted to the subscriber (e.g., shipper) via the docker image, so that the subscriber can ensure that the cargo is transported under the required conditions.

Table 1
Comparison of the IoT and blockchain.

a/a	Blockchain	IoT
1	Resource consuming	Most of the IoT devices are resource restricted
2	Complex process of block mining	Complex process of computation
3	Large networks restrict the blockchain system	The IoT is restricted by a large number of nodes
4	High bandwidth consumption in the blockchain	Bandwidth and resources are restricted

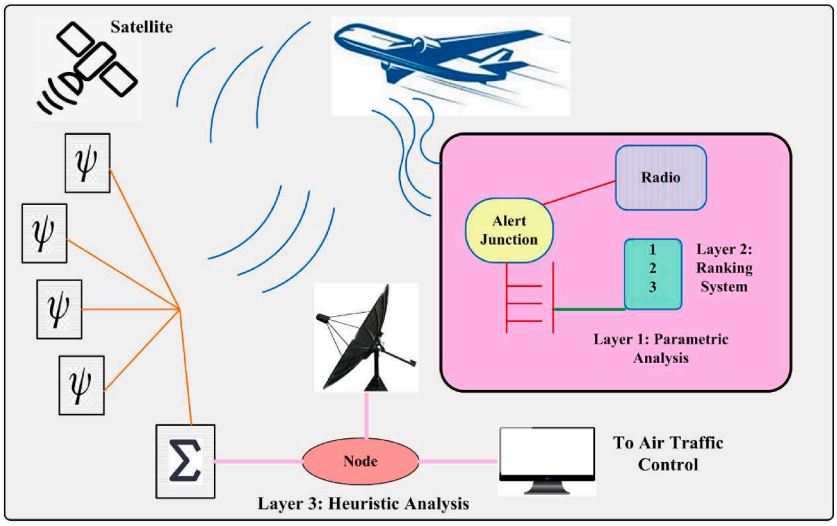


Fig. 10. Illustration of the AMELIA architecture.

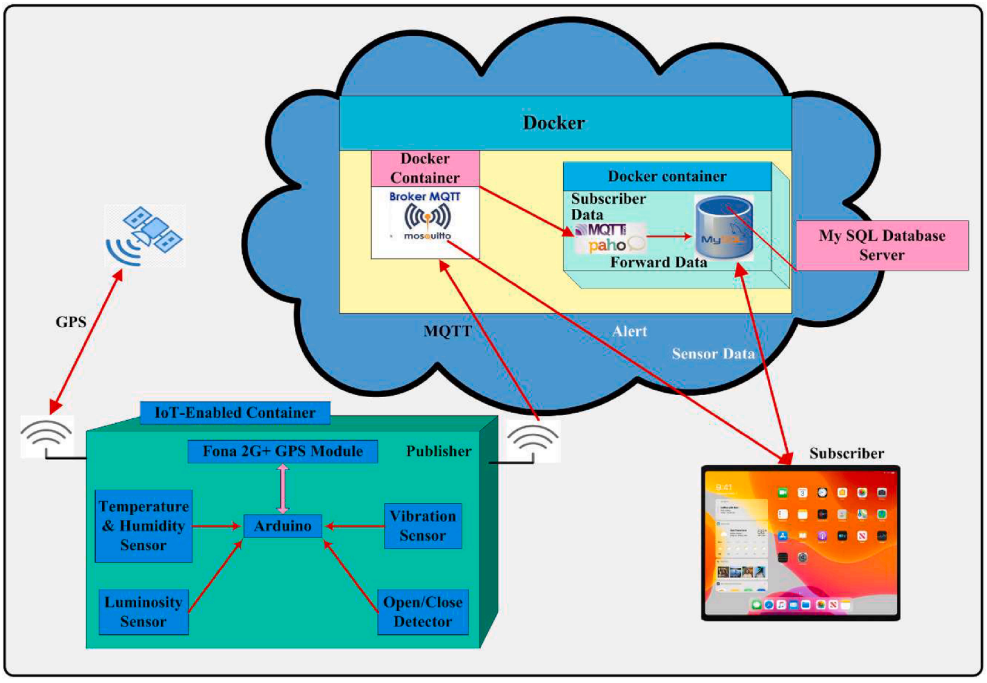


Fig. 11. Smart container system architecture in the shipping industry.

2.2.3. Manufacturing and industrial domains

Manufacturing industries make the largest connected IoT markets that comprise of several types of operations, services, products, and processes. Manufacturing is one of the industries that relies on the IoT technologies the most and has an enormous impact on people and economy. The IoT applications can improve services and product quality management (PQM), which involves control, planning, quality improvement, assurance, and enhancements, for complete life cycle of products, including advanced monitoring, tracking, and optimization (Zhong et al., 2017; Lampropoulos et al., 2018). Smart manufacturing, which is directly associated with the industry 4.0 concept, relies on the service-oriented architecture (SOA) and is deemed to be a unique model for manufacturing (Zhong et al., 2017). Fig. 12 illustrates the SOA structure for the IoT applications in manufacturing (Badarinath and Prabhu, 2017). The SOA is represented by several layers, including the sensing and data acquisition layer, network layer, service layer, and application layer. An effective interaction between the SOA layers is essential to ensure that the needs of end users will be satisfied. Many research efforts have been dedicated over the past years, aiming to improve multi-layer SOAs and attain higher standards (Ivezic et al., 2014).

Different manufacturing companies have different perception levels towards the deployment of IoT applications in their processes. Fig. 13 shows the acceptance level of the IoT technology by company size (PTC, 2018). It can be observed that approximately 44% of companies that use various Industrial IoT (IIoT) technologies have a net worth of less than $100 million. Only 13% of the companies have a net worth of more than $5 billion (PTC, 2018). Therefore, it can be concluded that the net worth of a company may directly influence its willingness to adopt different IIoT technologies. Smaller companies generally show greater interest in the IIoT which can be explained by their projections to grow after successful implementation of the IIoT technologies.

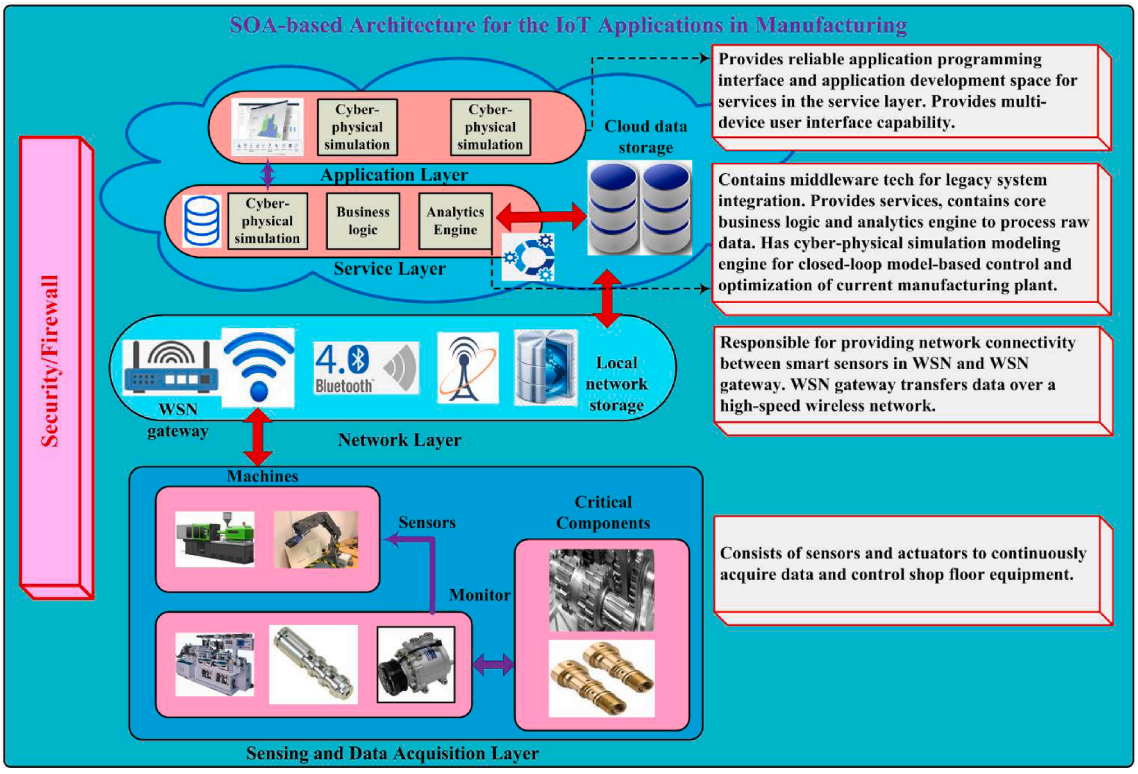


Fig. 12. The SOA structure for the IoT applications in manufacturing.

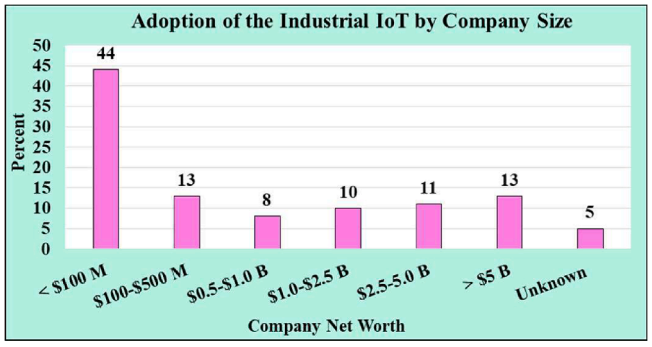


Fig. 13. Adoption of the Industrial IoT by company size.

2.2.4. Power management domain

With the growing demand for connected devices, the IoT networks are facing serious challenges that are associated with the network congestion issues. The problem becomes more complex when these devices either lose power or consume more power while transferring important data via the IoT networks. Currently, the IoT devices lack efficient power management and battery backup, while the data are being transmitted (Besher et al., 2021). A number of approaches have been proposed over the last years, aiming to ensure more effective user and device management, decrease device dormancy, and address power saving issues (Parvizimosaed et al., 2021). In case of conventional power grid systems, the concept of smart grid (SG) can be used to combine renewable and green technologies. The IoT-based technologies and embedded devices are used to enhance the SG effectiveness and facilitate intelligent decision making (Mehmood et al., 2021).

2.2.5. Healthcare and medical domains

The IoT has several applications in the healthcare and medical domains. These applications include mobile phones with RFID sensors for supervising delivery of medical services and medical attributes, use of sensors in combination, near field communications (NFC), ZigBee, 6LoWPAN, Bluetooth, Wireless Fidelity (WiFi), WirelessHART, and ISA100. Such applications can be effectively used to supervise measurements in blood pressure, blood sugar, body temperature, and levels of cholesterol (Sundmaeker et al., 2010). There exist IoT-aware healthcare-monitoring systems that were created using pre-existing technologies and can measure patient attributes (i.e., physical and psychological parameters) along with environmental conditions (Jimenez and Torres, 2015). With the growth of the internet and advanced IoT technologies, different wearable devices, such as health monitoring devices and smart watches, are available on the market and might be helpful in collecting health-related data which could be further used in early diagnostics of any medical condition (Darshan and Anandakumar, 2015).

As an example, Elhoseny et al. (2018) developed an IoT-based hybrid security model that can convert examined text data into medical images and enable secure transmission of medical data. The suggested model was created by combining a 2-D discrete wavelet transform 1 level (2D-DWT-1L) and a 2-D discrete wavelet transform 2 level (2D-DWT-2L) based on the steganography technique. Moreover, Islam et al. (2020) developed an IoT-enabled healthcare monitoring system that can be used to supervise not only the patient room conditions but also the primary health signs of patients as well. Fig. 14 shows the sensors capturing the data from a given hospital which is connected to ESP32 (a processing unit). This ESP32 device functions as a heart of the system when attached. It captures the relevant data and transmits the data to the IoT web applications. In order to have a cost-effective health monitoring, advanced IoT sensors and smart gateways are often used along with fog computing-based monitoring (Gia et al., 2017; Mutlag et al., 2019).

The IoT plays an essential role for the pharmaceutical industry as well. It is estimated that the AI in the U.S. healthcare market was around $320 million USD in 2016 and is expected to see a significant growth in the coming years. Of these investments, 35% account for the AI use in

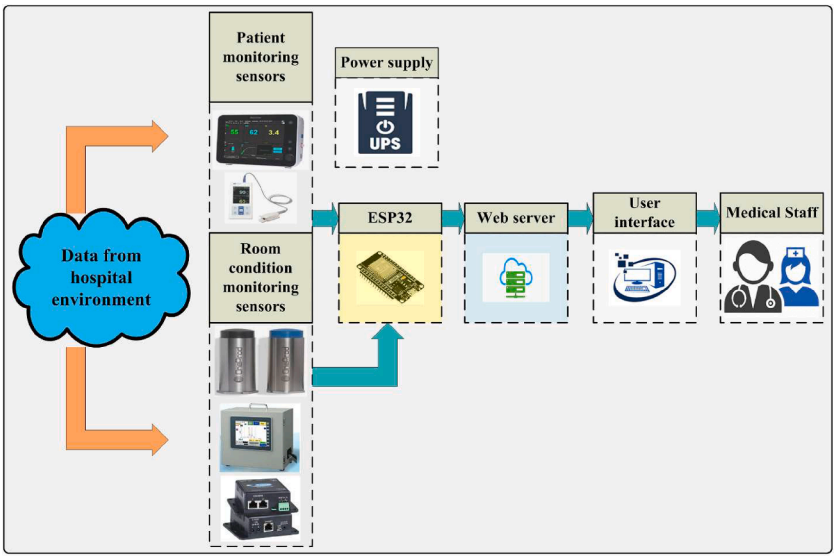


Fig. 14. Architecture of a smart healthcare monitoring system.

the discovery of drugs (Staines, 2018). Some of the common IoT-based applications in the pharmaceutical industry include (Alagarsamy et al., 2019): (1) automatic identification of objects and smart labeling of the objects; (2) capturing information and providing feedback; (3) equipment maintenance alert and forecasting; (4) 3D-printed drugs; (5) personalized medicine; (6) use of RFID for real-time logistic visibility; (7) use of sensors for collecting and reporting different attributes; and (8) warehousing and routing using smart IoT technology. The IoT-based technologies are actively used for manufacturing of pharmaceuticals, warehousing of pharmaceutical products, management of pharmaceutical supply chains, and product quality assurance. Similar to other domains, the IoT can be deployed for real-time supervision of processes involving pharmaceutical products (Sharma et al., 2020). Fig. 15 shows some of the key processes within pharmaceutical supply chains and how they can be integrated with the IoT applications.

2.2.6. *Commercial and consumer domains*

The IoT applications are common for many commercial domains and include items that are associated with businesses, such as device trackers, equipment control, inventory control, and larger infrastructure (e.g., smart cities, monitoring of large transportation systems, vehicle control, communications, and monitoring). Commercial IoT uses automation to coordinate and acknowledge any alteration in the commercial environment while minimizing the dormancy of system elements along with the associated operational costs. On the other hand, the consumer IoT applications include items used for personal and leisure activities, such as smart devices (e.g., phones and watches), tablets, intelligent home-connected devices (e.g., surveillance cameras, sensors, lamps, thermostat, etc.), and smart appliances (e.g., air conditioners, refrigerators, heaters, etc.). These applications can gather the relevant data and can be monitored and controlled remotely (Xenofontos et al., 2021). The IoT applications, blockchain technologies, and big data analytics have been also used in the tourism industry for different purposes, including but not limited to the following (Verma et al., 2021): (1) monitoring of tourism centers; (2) tourist behavior data collection and analysis; (3) tracking transportation movements between various attractions; (4) investigation of time and shopping habits; and (5) analysis of tourism-related expenses.

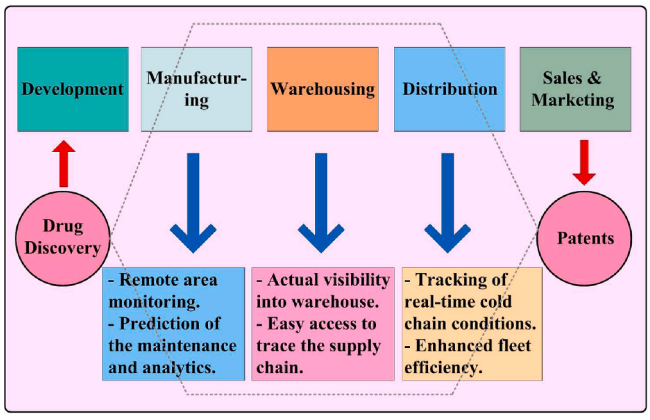


Fig. 15. Application of the IoT in various pharmaceutical supply chain processes.

2.3. *Current IoT trends in the railway industry*

The IoT-based smart railway market is projected to increase its market value from $15.85 billion in 2020 to $36.58 billion in 2026 with a compound annual growth rate of 15.14% (Mordor Intelligence, 2021). The increased growth in railways is likely to be directed predominantly by the increasing need for urban connectivity, growth in the IoT-based solutions and applications, as well as greater focus on decreasing emission levels. Based on the existing projections, freight movements are expected to increase by 150–250%, whereas passenger movements are expected to increase by 200–300% (Mordor Intelligence, 2021). Advanced IoT technologies, embedded sensors, big data analytics, and machine-to-machine technologies will pave the way for integrated intermodal transportation solutions to serve the growing demand for freight and passenger rail transportation. The total number of IoT-enabled devices is projected to significantly increase in various domains globally (see Fig. 2), including the railway industry as well. The railway-based IoT applications are expected to reach a $30-billion value in the next 15 years (Kimiagar, 2019). The following sections of the manuscript elaborate more on some of the key IoT-based applications that have been heavily used in the railway industry (also known as "Internet of Railway Things" – IoRT), including the following: (1) axle counters with temperature sensors and fiber optics; (2) monitoring of rolling stocks and level crossing safety; (3) IoT and big data-based railway inspection; (4) IoT-based perimeter intrusion detection systems; (5) AI-integration architecture for railways; and (6) IoT applications in maglev trains.

2.3.1. Axle counters with temperature sensors and fiber optics

Axle counters can detect vehicles at railway tracks and estimate the number of axles entering and exiting the tracks (SNCF et al., 2020). In case of an approaching train, the number axles entering and exiting the section should be equal, and no other vehicles should be allowed to enter this section. Therefore, axle counters play an important role in safe train operations. Furthermore, temperature sensors allow measuring temperatures of the locations where they are installed after every train passage. In case the detected temperature crosses a particular threshold, the train will be stopped at the consecutive railway station in order to prevent the inflammation of cargo, rolling stock, and surrounding environment as a result of sparks and excessive heat. The deployment of temperature sensors allows avoiding accidents due to overheating of bearings. Effective monitoring of the track-side environment can be accomplished by means of fiber optic sensing (FOS). The FOS has various detection capabilities, including track blockages due to landslides, point machine diagnostics, train derailments, cable theft, and flat spots on train wheels (SNCF et al., 2020). A fiber optic cable should be added to the cable duct which is running alongside the railway track in order to enable the FOS operations. The cable with a length of up to 40 km can be connected to the detection unit that is located close to the cable duct (see Fig. 16). Variations in light rays can be used by sensors within the detection unit in order to determine particular events and trigger alerts.

2.3.2. Monitoring of rolling stocks and level crossing safety

The Société Nationale des Chemins de Der Français (SNCF), the French railway company, launched the "Télédiag" program which aims to make substantial improvements in the railway maintenance process. The program is inspired by a wide range of modern technologies, including the IIoT, big data analytics, edge computing, and cloud computing, that allow collecting real-time information for predictive and preventive maintenance (SNCF et al., 2020). Furthermore, Télédiag can be used for the rolling stock remote quality control as well. A significant amount of the IoT information can be gathered for the rolling stock equipment, such as state-of-charge for backup batteries, sandbox monitoring, water level monitoring in tanks, and door state monitoring. The IoT-based systems have been also used to monitor the state of level crossings, where there is a risk of potential conflicts between vehicles and trains at the same elevation. Level crossings generally record a significant number of vehicle-train collisions and pose safety concerns to highway and rail users. The IoT-based applications can be used to remotely monitor irregular activities at level crossings and send the appropriate notifications to the train driver and network control center (see Fig. 17).

2.3.3. IoT and big data-based railway inspection

The big data along with the IoT applications have lately become a promising alternative in improving productivity and reliability of the existing railway inspection system. Such a trend can be supported by the recent development in the information technology (IT) and advanced sensors (Zarembski, 2014). Presently, huge amounts of railway inspection-related data are gathered using various devices, such as ultrasonic probes, video cameras, eddy current probes, and acoustic emission transducers. Modern approaches for big data analytics assist with the evaluation of big data and provide effective guidelines for railway inspection (Li et al., 2017). Fig. 18 illustrates how the IoT and big data can be used for railway inspection. The sensing function is executed in the first step using the appropriate on-site and on-board equipment units. Then, the sensing data are collected and processed in the second step. In the third and the last step, the processed data are used to develop advanced models for planning railway maintenance.

2.3.4. IoT-based perimeter intrusion detection systems

Modern perimeter intrusion detection systems are based on the IoT framework and rely on data-fusion algorithms. There are alternative approaches for detecting perimeter intrusion at railways (e.g., vibration cables, leaky coaxial cables, microwave walls, active infrared, fiber-optic vibration, ANENC, video surveillance, etc.) which have some limitations. Advanced IoT-based perimeter intrusion detection systems demonstrated satisfactory performance not only under normal conditions but also under adverse weather conditions as well. Fig. 19 illustrates an IoT-based perimeter intrusion detection system for railway applications. The system has a total of three layers of architecture (Xie and Qin, 2019): (1) perception layer which is a core layer of the framework and is responsible for information acquisition; (2) network layer which is the middle layer of the framework and is responsible for data transmission; and (3) application layer which is the top layer of the framework and is responsible for data processing. Note that the perception layer may include some of the alternative perimeter intrusion detection systems (e.g., fiber-optic vibration, advanced types of sensors). Other prototype of obstacle detection systems is based on three ultrasonic sensors. Of the three sensors, the first sensor is installed in the front of the prototype, and the other two are placed on either side of the prototype. The data gathered by the sensors are further processed and transmitted to the cloud server.

2.3.5. AI-integration architecture for railways

The main aim of integrating the AI in railway operations was to analyze the potential of AI in railway applications and prepare a future roadmap for developing the next generation signaling systems, network management, and operational intelligence. Fig. 20 illustrates the integration of AI with railway operations. It can be observed that a variety of AI-based techniques can be used specifically for railway operations, such as computer vision, optimization, big data analytics, explainable and trustworthy AI, machine learning, and formal reasoning. Many problems associated with railway operations have high computational complexity (e.g., timetabling, real-time rescheduling of the available resources).

Advanced AI-based methods, such as heuristics, metaheuristics, and customized exact optimization methods, were found to be effective in solving decision problems of high complexity in a timely manner (Dulebenets, 2018, 2019; Safaeian et al., 2019; Fathollahi-Fard et al., 2021a; Gholizadeh et al., 2021; Theophilus et al., 2021; Pasha et al., 2022a). The AI integration involves the following major components

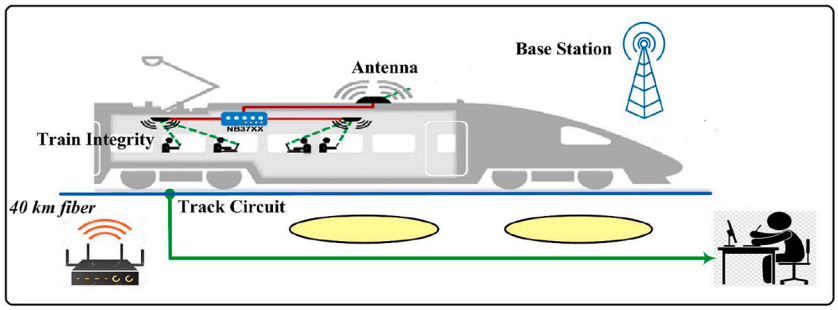


Fig. 16. Track-side monitoring using fiber optics.

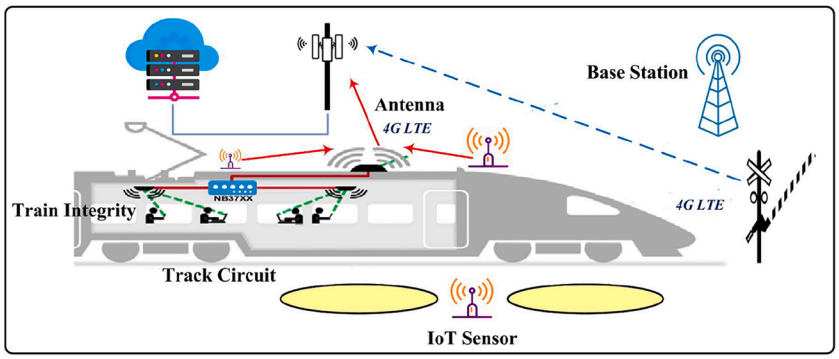


Fig. 17. Level crossing monitoring using the IoT.

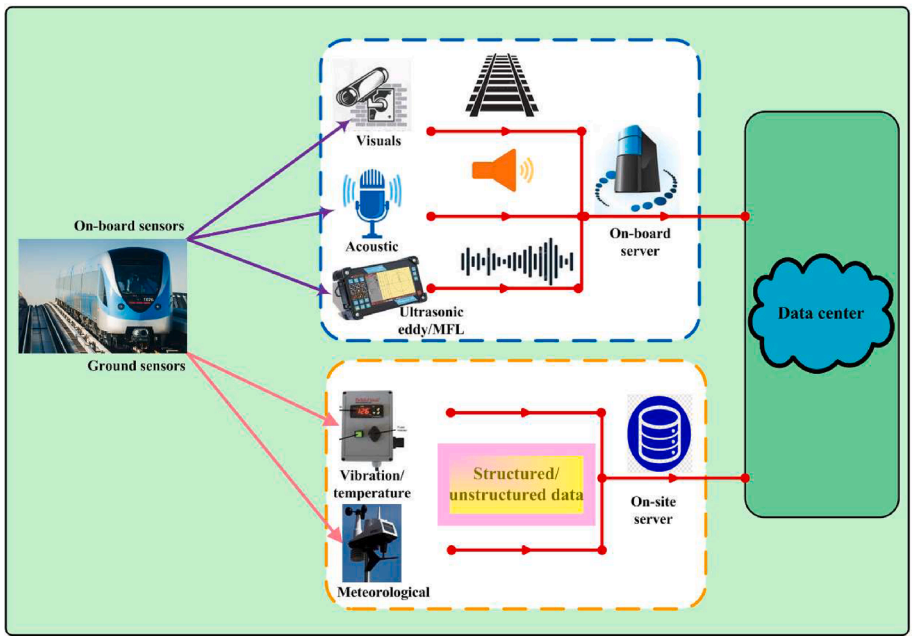


Fig. 18. Railway inspection using the IoT and big data.

(Flammini et al., 2020): (1) taxonomy and AI state-of-the-art for railways and related sectors; (2) AI for railway automation and safety; (3) AI applications for defect detection and predictive maintenance; (4) AI for traffic management and planning; (5) dissemination activities and identification of future directions; and (6) project management.

2.3.6. *IoT applications in maglev trains*

Maglev trains have received increasing popularity due to their comfort, advantages of no friction, and low noise (Sun et al., 2020). The IoT-based applications are actively used in maglev trains. The IoT allowed improving safety of maglev trains and passengers to a significant extent. Fig. 21 shows the IoT-based operations of maglev trains and major components involved. The special remote data acquisition and transmission equipment is used to transmit the train status data, weather information, and emergency diagnostics information directly to the maglev train. The hardware for remote data acquisition and transmission equipment primarily relies on a F28075 chip which has high running speed and abundant peripheral ports (Sun et al., 2020). All the collected data are further stored in a designated database. Exclusive diagnostics and monitoring software are used to analyze and display the data to the appropriate personnel. The appropriate personnel can review the data and evaluate the working state of a given maglev train. When necessary, a specific suspension control strategy can be deployed by the personnel to enhance (or even optimize) the overall performance of the magnetic suspension system of the maglev train.

3. Review of the relevant state-of-the-art efforts

This survey study primarily focused on the state-of-the-art research efforts related to the applications of IoT in railways, emerging IoT technologies, IoT implementation challenges, IoT technologies for improving level crossing safety, current trends and future research needs associated with the IoT deployment in railway operations and other closely related fields. A comprehensive up-to-date review of the relevant literature was performed in this study based on the content analysis method that is viewed as a well-known methodology for systematic reviews of the scientific literature (Wester and Krippendorff, 2005). A thorough search for the relevant scientific literature was performed using various scientific databases, such as IEEE Explore, Web of Science, Science Direct, Springer Nature, ACM, Wiley Online Library, and Google Scholar. The search was performed using the following keywords and phrases: “Internet of Things”, “IoT and railways”, “IoT technologies in railways”, “IoT challenges”, “IoT advantages”, “rail automation challenges”, “future communication technologies”, and “IoT applications in different domains”.

The search resulted in thousands of scientific studies; however, only the articles that are most relevant to the theme of the IoT applications in the railway industry and other closely related fields were selected for a

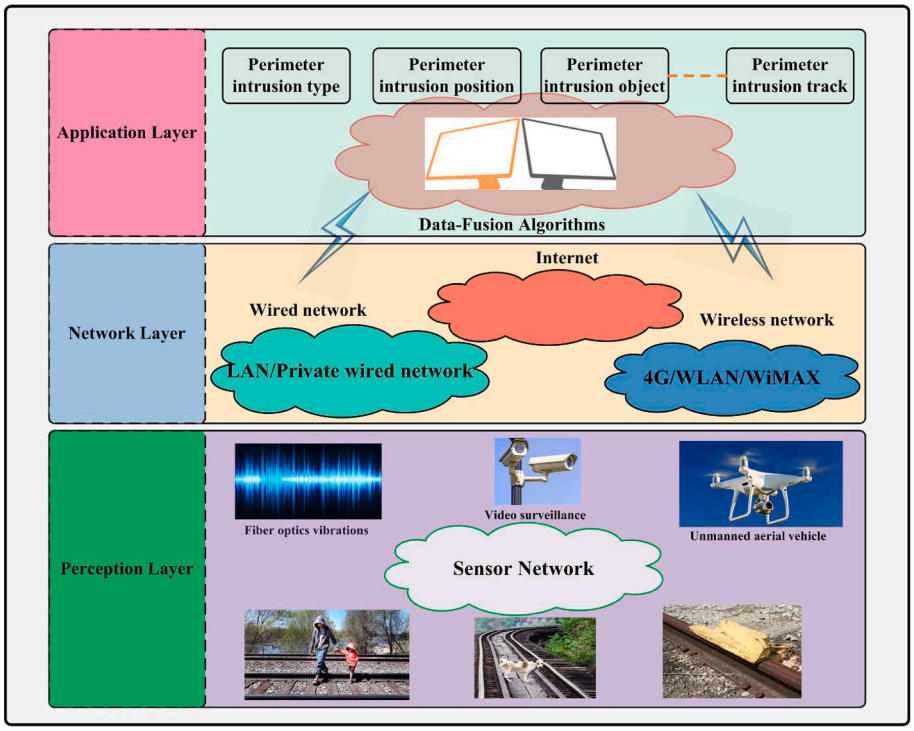


Fig. 19. The IoT-based intrusion detection system for railway applications.

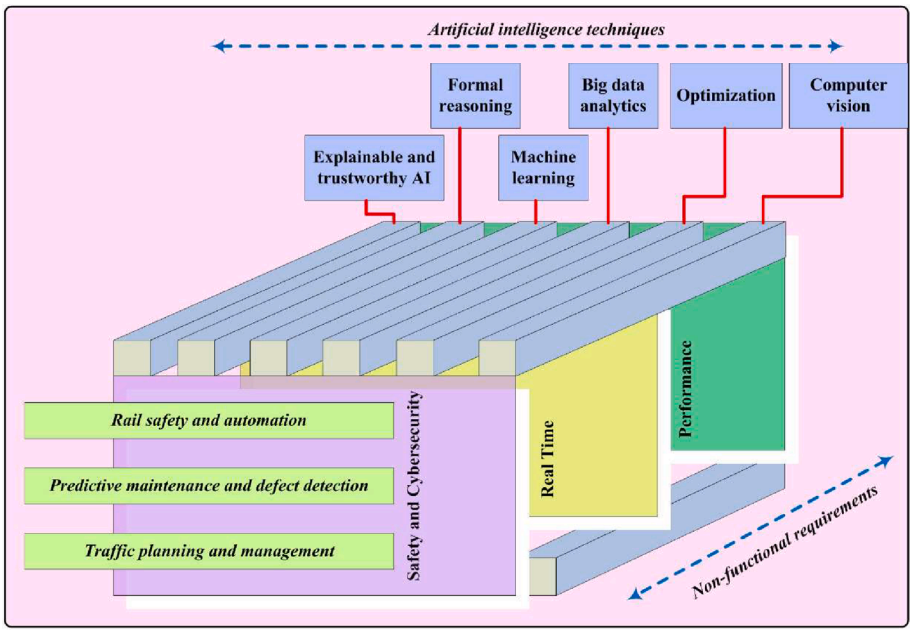


Fig. 20. Integrating the AI in railway applications.

detailed review. Some relevant articles discussing futuristic technologies (e.g., 6G and 7G) that have the potential of improving railway management and ensuring sustainability of operations in the following years were also considered. The collected studies on the IoT applications have been classified into the following categories: (1) IoT applications for sustainable railway management and operations; (2) IoT applications at level crossings; (3) green IoT applications; (4) general studies on the IoT technologies and applications; (5) emerging communication technologies; and (6) IoT challenges. The following sections of the study present a description of the collected studies.

3.1. IoT applications for sustainable railway management and operations

A variety of railway-specific IoT applications have been developed over the past years, aiming to improve sustainability of railway management and operations. For example, Liu et al. (2010) explored potential advantages of using the IoT in the railway industry. The study proposed a real-time tracking application that could be used to monitor the state of the goods throughout transportation by rail. Furthermore, the developed method attempted to facilitate docking between the rail and road modes and ensure efficient door-to-door transport which could

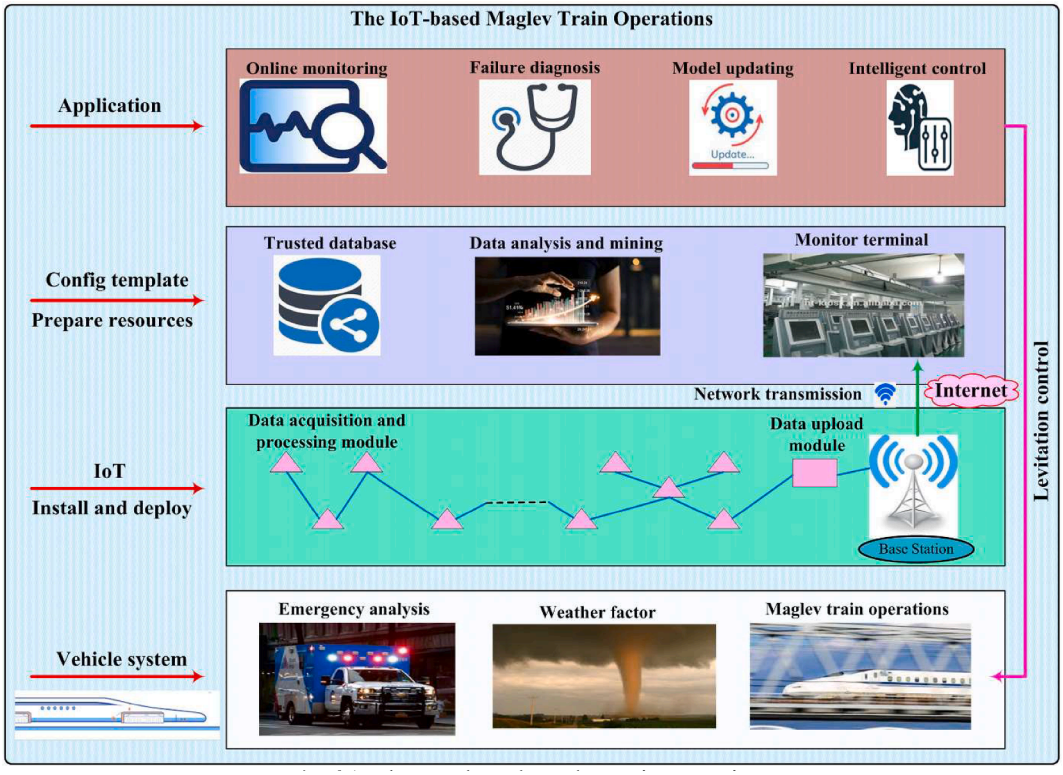


Fig. 21. The IoT-based maglev train operations.

further enhance the competitiveness of rail transportation. Zhang et al. (2011) studied the IoT deployment for the Chinese railway system. It was indicated that the IoT-based technologies could assist with a variety of operations, including train tracking and positioning, automatic fare collection, security early warning, station train information sharing, cargo management, and warehouse management.

Zhang (2012) studied the deployment of various IoT technologies (e.g., RFID tags, sensors) for maintenance, repair and operation of high-speed trains. It was indicated that the IoT could be used to identify defects of trains in real time and transmit safety alerts when needed. Moreover, the IoT technologies could collect and process the relevant data to ensure proper maintenance of trains throughout the entire life cycle. The study underlined that the IoT could improve maintenance efficiency, reduce labor intensity and failure likelihood. Lei et al. (2013) indicated that effective information perception, processing, and sharing is essential to improve the existing railway transportation services in China. The IoT-based technologies could be effectively used for the railway information integration. The study proposed an IoT-based framework which included a perceptual recognition layer, access layer, carrying network layer, application controlling layer, and intelligent application layer. Ling (2013) pointed out that rail transportation safety could be improved by means of deploying the IoT-based technologies, including RFID, infrared alarms, fire alarms, and a maintenance management system for the key devices. Application of intelligent IoT devices would prevent freight theft issues, reduce fire hazards, ensure proper maintenance monitoring and inventory management, as well as improve economic benefits of safety.

Shi and Wang (2013) underlined that the IoT development could positively impact the flow of railway information. An intelligent railway information platform was established which relied on the basic environmental layer, integrated IoT application layer, application support layer, and railway transportation application layer. It was concluded that the suggested platform could substantially improve railway operations. Zhang and Shao (2013) presented an IoT-based architecture for railway safety monitoring in China. The developed architecture included a total of three layers, including the sensing layer, network layer, and application layer. Despite substantial IoT advantages for railway safety monitoring, it may take a significant amount of time before the IoT technologies would be heavily deployed on railway segments. Li et al. (2014) assessed the challenges associated with the mass passenger flow in the Beijing rail transit network (China). The study proposed an IoT-based system for mass passenger rail transit that relied on information sharing, real-time sensing, and intelligent analysis. It was found that the proposed methodology was able to accurately forecast the capacity required for mass passenger flow and assist with effective rail transit management.

Ai et al. (2015) indicated that the future development of railway transportation systems would require interconnection between the major elements involved (e.g., trains, goods, travelers, infrastructure). The study proposed a wireless communication network that relied on the multiple-input-multiple-output (MIMO) concept for train cars and railway stations. The suggested methodology is anticipated to meet the requirement of high spectrum and high-data-rate efficiency. Eiza et al. (2015) suggested a communication model which was named as "RIoT" (Rail Internet of Things) to enhance railway services and discussed the user needs. The RIoT system included a number of components, such as trains, tracks, stations, passengers, and rail control center. The study also outlined potential security risks for the RIoT and proposed certain countermeasures (e.g., encryption of communication channels, risk analysis for the available devices). Chapman et al. (2016) highlighted that low adhesion could be a major issue for railways as it could decrease acceleration and braking efficiency. The study proposed an emerging IoT-based technology for high-resolution cost-effective rail moisture monitoring network. Moreover, the suggested low-cost sensor was found to be superior to the existing more costly sensors after both laboratory and field experiments.

Gangwar et al. (2017) suggested a new IoT-based system for passenger service and comfort in rail transportation. The system relied on a Bluetooth Low Energy technology to determine the exact locations of crew members inside the train. A multi-objective optimization algorithm

was developed to allocate the available crew members for service of passengers, considering the information regarding location, service arrival time, and workload factor. The proposed approach was found to be superior compared to the traditional centralized method. Jo et al. (2017) presented a low-cost IoT solution for smart railway infrastructure which included the gateway, IoT network, device platform, and platform server. An in-depth case study was performed to evaluate the proposed methodology. It was found that the developed IoT-based solution was able to easily handle the condition information for the railway infrastructure.

Li et al. (2017) mentioned that the IoT-based technologies (e.g., sensors, advanced computing technologies, big data, and cloud computing) could be used to meet the growing demand for railway transportation. The authors presented the architecture for smart railways that included a total of four layers: (a) perception and action layer; (b) transfer layer; (c) data engine layer; and (d) application layer. It was recommended that the railway operators should focus more of the development of smart railway technologies to enhance safety and efficiency of the railway network. Zheng et al. (2017) highlighted an increasing use of the IoT technologies in railway operations and the need for maintaining information security. The study proposed an authenticated encryption scheme that could protect confidentiality and integrity. The conducted analysis demonstrated that the developed method was able to guarantee an appropriate security level.

Karaduman et al. (2018) suggested a methodology for the IoT-based condition monitoring of railway operations. The proposed methodology relied on cameras that were monitoring dedicated railway segments and taking images which were further transmitted to a central computer. The appropriate image processing techniques were used to evaluate the obtained images and take the required actions when needed. Naser (2018) studied the blockchain and its potential applications related to the railway industry. The study highlighted that the blockchain could assist with addressing security issues as well as the challenges associated with the data integration. It was pointed out that the blockchain applications had only a moderate adoption rate in the railway industry which does not allow full exploration of their benefits. Saghafi and Kordsalari (2018) aimed to determine the required driving forces that could facilitate the IoT deployment on the Iranian railways. The authors conducted a set of environmental surveys and interviews with the industry experts. A number of challenges in the IoT deployment were identified (e.g., old infrastructure, equipment theft, resistance to change, sanctions, conflict of interest for certain stakeholders, technological illiteracy, cost, moral indifference). The identified driving forces were classified into different groups, such as technological, economic, environmental, political, etc.

Sneps-Sneppe and Namiot (2018) suggested the deployment of 5G technology for urban railways, aiming to ensure reliable connectivity for efficient, safe, and attractive railway services. The Moscow urban railway project was considered as a practical example. It was indicated that high-speed railway services were needed to support physically separated territories. Castillo (2019) underlined that rail automation has the potential of reducing risk factors caused by humans. The study discussed the deployment of IoT-based technologies in autonomous rail transportation. It was indicated that the IoT technologies would allow achieving all the benefits from automation without affecting safety in a negative way. Nevertheless, some IoT limitations were pointed out as well (i.e., limited connectivity and bandwidth). Ganga et al. (2019) proposed an IoT-based methodology for passenger rail services, aiming to consider passenger comfort criteria. The requests from passengers (e.g., medical services, blanket services, catering services, emergency issues) were allocated among the available crew members based on the established priority schedule. The work orders of crew members were recorded in a separate database. The suggested approach was compared to the conventional method and was found to be superior.

Shankar et al. (2019) explored the use of IoT technologies for detection of cracks in rail tracks and major landslides in hilled areas. The proposed system could detect the existing hazards and transmit the information to the nearest station. The authorized personnel could further use the obtained information and take the appropriate actions to prevent train accidents. Xie and Qin (2019) designed an IoT-based framework for perimeter intrusion detection at high-speed railways. The framework relied on the integration of different sensors. A custom data-fusion algorithm was presented to process the data collected from multiple sensors and improve the detection accuracy. The experiments demonstrated the efficiency of the proposed methodology under normal and inclement weather conditions. Ai et al. (2020) pointed out that the 5G technologies could substantially improve high-speed railway operations and meet the expectations related to safety, mobility, comfort, reliability, and transparency. A network slicing architecture was proposed for the 5G high-speed railway system. Based on the conducted experiments, significant 5G-based key technologies were identified, including fast channel estimation, spatial modulation, wireless backhaul, enhanced handover strategies, among others.

Arunjyothi and Harikrishna (2020) pointed out that there is a rapid development of the IoT-based technologies (e.g., multiple local connections and software, radio blaze, hardware-related marketing), but managing the IoT connections is still a challenge. The authors introduced a new network architecture to improve the efficiency of radio access technologies in the railway field conditions. Dirnfeld et al. (2020) discussed Low-Power Wide-Area Networks (LPWAN) with a specific emphasis on smart railways. It was underlined that both IoT and LPWAN would be very promising technologies for cost-effective remote monitoring, surveillance, and control over large geographical areas even in case of situations where the power supply is restricted. Flammini et al. (2020) analyzed the prospects of integrating the AI in railway operations through the project named “RAILS”. The project is expected to improve maintainability, reliability, security, safety, and performance. The AI technologies would be efficient in addressing certification issues and emerging threats. The advanced AI algorithms are also anticipated to assist with a variety of challenging decision problems that are common for daily railway operations.

Mohamed et al. (2020) developed an integrated maintenance logistics monitoring system for high-speed rail which was inspired by the IoT concepts. A custom algorithm was designed to prevent RFID tag-reader collisions. The results from experiments demonstrated that the presented system could be effective to ensure adequate maintenance activities and assist with a timely response to urgent repair orders. Sun et al. (2020) studied the use of IoT technologies in maglev rail transit systems. The research suggested an IoT-based adaptive fuzzy controller for supervising medium to low-speed maglev trains. The effectiveness of the proposed methodology was assessed based on the experiments conducted for a full-scale maglev train. The developed methodology was found to be feasible and efficient.

3.2. IoT applications at level crossings

Level crossings (or “highway-rail grade crossings”) represent locations, where there is a conflicting point between vehicles and trains at the same elevation. There is always a risk of collisions between trains and vehicles at level crossings (Abioye et al., 2020; Kavoosi et al., 2020b; Pasha et al., 2021; Singh et al., 2021b). The IoT-based technologies could be one of the solutions towards safety improvements at level crossings. Dhande and Pacharaney (2017) studied level crossing safety at unmanned crossings with a primary focus on the detection of faulty tracks. The study proposed an IoT-based system which included sensors, Global System for Mobile Communication (GSM), and Global Positioning System (GPS). The developed system was found to have a variety of advantages, including low cost, low power, high accuracy, and timely data analysis. Minoli and Occhiogrosso (2017) underlined that a significant number of fatalities are reported at level crossings every year. The study proposed an IoT-based approach for sending alerts due to static and dynamic rail track intrusions at level crossings. The developed method could be potentially integrated with the positive train control

system and automatically stop an incoming train when necessary. Potential IoT-related cybersecurity issues were discussed as well.

Virtanen et al. (2019) discussed the safety challenges that are associated with autonomous vehicles approaching level crossings. It was pointed out that the perception sensors of autonomous vehicles, vehicle-to-everything messaging, and train-tracking solutions could facilitate safe passage of vehicles through level crossings. Dedicated short-range communications (DSRC) can be used to communicate the information between the approaching train and road-side units in the vicinity of level crossings (see Fig. 22). The road-side units can further transmit the information to the autonomous vehicles in the vicinity of a given level crossing to ensure that there will not be any conflicts with the approaching train. Aziz et al. (2020) presented a methodology that can be used for detecting the objects on railway tracks and their vicinity (e.g., vehicles entering level crossings). Two main elements were used to monitor the objects and collect the data. The first element was represented by the IoT system for monitoring and storing the data regarding the objects in the vicinity of rail tracks. The second element was represented by the radar and processing software to display the distance between the objects and the device.

Ranjith and Vijayaragavan (2020) pointed out that many level crossings in Tanzania are not automated which causes delays and increases the risk of accidents. The study proposed the IoT-based mechanisms that can operate automatically without any human involvement. The proposed system was found to be effective in improving level crossing safety and promoting smart railway transportation. Singh et al. (2020) suggested an automated vehicle detection system using the IoT technology. The study provided a detailed review of numerous challenges and issues related to automatic vehicle detection at level crossings. The proposed vehicle detection system is likely to enhance traffic control at level crossings and decrease the number of accidents.

Prasad and Madhumathy (2021) suggested a new IoT-based system which relies on different sensors and can be used for railway maintenance. The IoT system could prevent major accidents or alleviate the associated effects in case of the accident occurrence (e.g., train derailment in the vicinity of level crossings). It was pointed out that the proposed system could be vulnerable due to hacker attacks. Therefore, a one-time password was adopted for security purposes. Talpur et al. (2021) pointed out that efficient gate opening and closing operations are essential for level crossings. The study proposed force-sensitive resistor detectors for automatic side road crossing protection. The proposed system could directly communicate with the nearest control room in case of unexpected situations. Furthermore, sonar sensors were adopted to identify the objects that may potentially appear in front of an approaching train. The suggested IoT technologies are expected to effectively monitor the level crossing conditions.

Singh et al. (2021a) discussed various technologies, including the IoT-based applications, that can be used for autonomous trains. A specific emphasis was given to safety issues at level crossings. It was indicated that advanced IoT technologies (e.g., DSRC technologies) would prevent potential conflicts between autonomous vehicles and autonomous trains which would further increase safety of users at level crossings. A number of other studies have been conducted to introduce and evaluate various communication technologies that could potentially improve level crossing safety and prevent collisions between vehicles and trains (Hsu and Jones, 2017; Zaouk and Ozdemir, 2017; Voege et al., 2017; U.S. DOT, 2018; Neumeister et al., 2019; U.S. DOT, 2021).

3.3. Green IoT applications

Several studies were performed to assess the environmental benefits from the IoT applications in the railway industry and other relevant domains. Fraga-Lamas et al. (2017) investigated potential advantages of the commercial IIoT for the railway industry. The study analyzed the recent efforts related to smart infrastructure, predictive maintenance, video surveillance systems, advanced monitoring of assets, railway operations, train control systems, safety assurance, and signaling systems. A specific emphasis was dedicated towards the internet of smart trains that encompasses various elements (see Fig. 23). Furthermore, the issues surrounding cybersecurity and energy efficiency were mentioned as well. It was pointed out that emission reduction could be achieved by optimizing train timetables, use of energy storage devices, smart metering methods, and optimized train trajectories.

Adebiyi and Cruz (2018) evaluated the existing IoT-based green

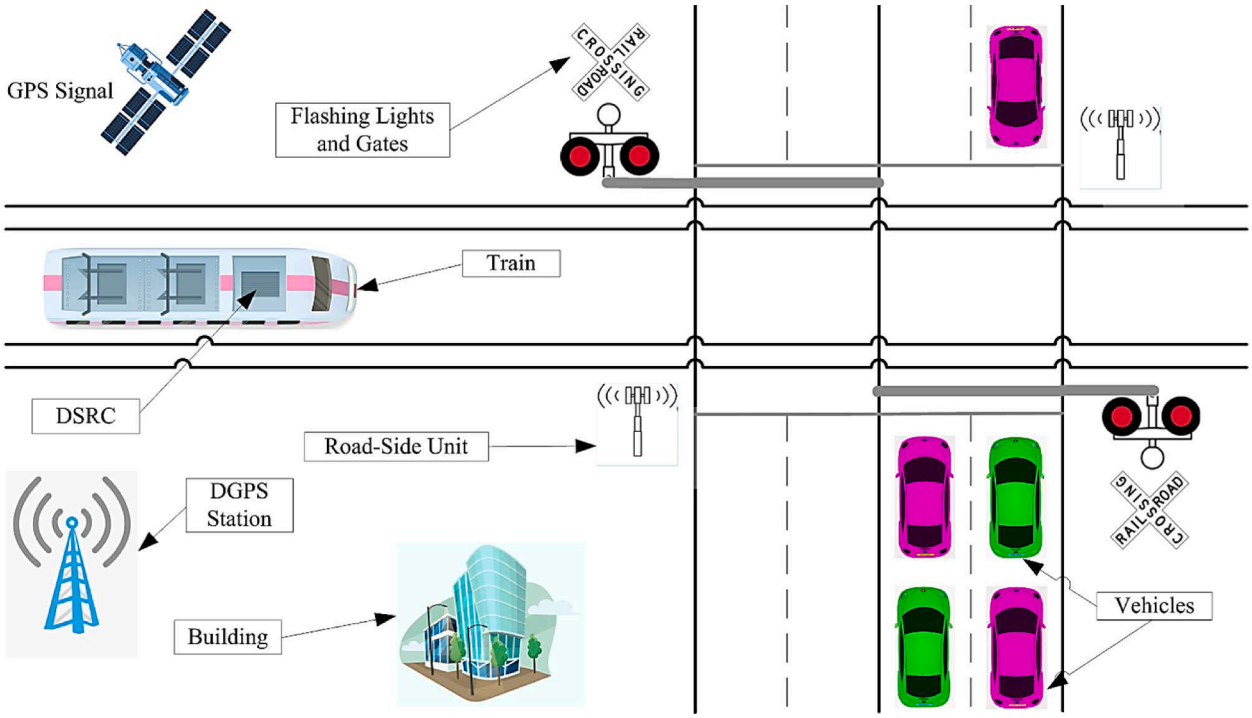


Fig. 22. Communication technologies at level crossings.

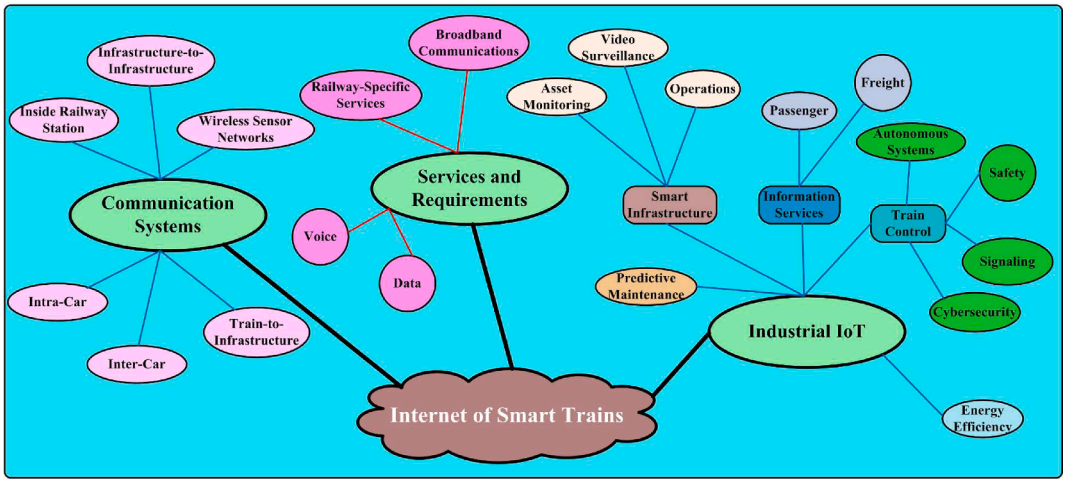


Fig. 23. Internet of Smart Trains.

sustainability technologies for the railway industry in Malaysia. It was underlined that the IoT improved the operational efficiency of railway transportation systems, enhanced automation, and allowed better passenger experience. However, additional considerations should be given to adequately address the green and sustainable development goals (e.g., improved management, decarbonization, reduced energy consumption, better utilization of the available assets). The study proposed a strategic plan to facilitate green and sustainable development of the railway industry in Malaysia. Elmustafa and Mujtaba (2019) discussed the concept of "smart environment" that is associated with the deployment of IoT technologies to address a variety of environmental problems, including: (1) the quality of water and health; (2) air pollution; (3) weather; (4) monitoring of radiation; (5) waste management; and (6) natural disasters. The IoT could assist with sensing, monitoring, and tracking the objects of environment which can further facilitate green and sustainable lifestyle.

Perwej et al. (2019) underlined that the European Union set a quite challenging target for reducing the greenhouse gas emission levels. It was indicated that the IoT applications could be effectively used to measure the emission levels in different parts of the city (e.g., metro stations, crowded areas, parks, etc.). The data regarding pollution levels can be collected from the IoT devices and shared with the public, so necessary actions can be undertaken to provide sustainable solutions for the areas with high pollution levels. Solanki and Nayyar (2019) investigated the principles, applications, technologies, and projects associated with the implementation of green IoT (G-IoT) in different domains. The G-IoT applications are expected to overcome the limitations of the existing technologies in terms of emissions, energy waste, excessive use of fuel, and greenhouse effects. The study also discussed various challenges of implementing the G-IoT in the real world.

Zantalis et al. (2019) conducted a comprehensive review of the ML and IoT applications in smart transportation systems. The study pointed out that ML and IoT could assist with route optimization. Optimized transportation routes are expected to minimize traffic congestion at busy roadway and rail corridors and decrease the associated emissions produced by vehicles. The ML and IoT applications could also facilitate timely arrivals to the intended destinations. Mehmood et al. (2021) discussed the potential of integrating IoT with edge computing and smart grid. Smart grid can provide green and renewable energy solutions for smart cities (including smart transportation systems), and its efficiency can be substantially augmented with the new technologies (i.e., IoT, edge computing, big data, and artificial intelligence). The IoT applications could assist with the collection of data with high resolution. Edge computing, on the other hand, would address the issues of data security, privacy, latency, and high band utilization.

Zhong et al. (2021) discussed the key IoT technologies that would be critical for the further development of high-speed railway systems. The study proposed an IoT-based architecture for high-speed railways that included a total of four layers, such as the perception layer, network layer, platform layer, and application layer. It was concluded that the IoT deployment could improve environmental sustainability of high-speed railway systems, along with enhanced safety, efficiency, and comfort.

3.4. *General studies on the IoT technologies and applications*

Several studies discussed the deployment of various IoT technologies as well as IoT applications in different areas which could be extended to the railway industry and improve sustainability of railway operations. Sundmaeker et al. (2010) described the Cluster of European Research Projects on the Internet of Things (CERP-IoT) which included a total of 30 major research initiatives in the field of advanced technologies (e.g., sensing technologies, detection technologies, and RFID). The study discussed the current IoT deployment efforts in various countries as well as the existing IoT challenges. The number of IoT connected devices was projected to grow significantly in the following years. Economides (2016) suggested an IoT-based model to address user perception towards the IoT technologies. The proposed model directly considered user characteristics (e.g., age, gender, education, and experience with computers). The study divided different IoT services and applications into three major domains, including personal, business, and public. Furthermore, some major IoT-related challenges were discussed as well (i.e., technology, social, business, and human).

Bali et al. (2018) discussed different applications of the IoT, such as smart cities, offices, homes, transportation, interoperability, vegetable tracking systems in the agriculture sector, cybersecurity, and e-commerce. The study also described the middleware which serves as a software layer between different IT infrastructures and is able to hide technical programming details. It was also pointed out that the external environmental factors (e.g., temperature) could significantly influence the IoT services. Chapman and Bell (2018) investigated the potential of IoT applications for monitoring the impacts of weather and climate on infrastructure. It was underlined that low-cost IoT sensors showcase adequate performance in the field and laboratory settings. However, age of the technology could affect the accuracy of collected data. Another challenge was found to be annual calibration and maintenance. Bansal and Lal (2019) indicated the growing interest towards the IoT technologies that can be integrated with Wi-Fi, Bluetooth, and RFID for connecting a wide network area (wired or wirelessly). The study mentioned that the IoT could improve quality of life, as many devices could be

automated and more efficient energy utilization might be achieved. A set of important IoT application areas were underlined, including smart cities, buildings, and homes.

Gharami et al. (2019) discussed the significance and different approaches being used by the IoT. The study also described some of the major areas where the IoT has gained its prominence and a variety of new methodologies that could be implemented. However, the authors specifically indicated that one of the main obstacles behind the broad IoT implementation is the lack of compatible devices along with the security and privacy issues. Chen (2020) discussed an increasing use of visual sensors in the IoT-based systems due to their capability to provide richer information. The integration of visual sensors with the traditional IoT technologies led to a new paradigm named as "the Internet of Video Things (IoVT)". It was indicated that the new characteristics of the IoVT are expected to impose additional requirements and challenges to the existing infrastructure. A self-learning capability was found to be the major feature that would be essential for the future IoVT technologies. Adil and Khan (2021) provided a comprehensive review of the Healthcare IoT (H-IoT) applications for sustainable smart cities under the COVID-19 settings. The study highlighted substantial effects of the COVID-19 pandemic on healthcare systems across the globe. It was indicated that the H-IoT systems are complex and are represented not only by cluster heads, sensors, controls, and base stations but also by humans (nurses, patients, and pharmacists).

Mehmood et al. (2021) pointed out that the efficiency of smart grid could be increased with smart embedded devices that would enable intelligent decision making (e.g., the IoT-based technologies). The study proposed to use the edge computing technologies for the IoT-enabled smart grid to address the security, latency, privacy, and high bandwidth utilization issues. Pal et al. (2021) indicated that the IoT systems deal with large volumes of data which are often sensitive (e.g., the data related to financial, health, location, and other personal attributes). The authors reviewed the recent trends in the development of blockchain solutions for the IoT access control. Several blockchain attributes, such as secure storage, decentralized control, and information sharing, were found to be essential for the IoT access control. Wang and Sarkis (2021) discussed the existing trends and future research needs in digitalization of freight transportation. The authors categorized the existing digitalization trends into: (1) connecting; (2) collaborating; and (3) capitalizing. Some of the major technologies were discussed for each category to show how these technologies could create significant changes in supply chains and logistics systems.

A number of studies did not investigate the IoT-based applications specifically for rail transportation but focused on other relevant domains (e.g., supply chain management, automotive industry, manufacturing industries) and/or interactions between various domains. However some of the findings and outcomes from the conducted studies could be potentially useful for the railway industry. For example, Yi and Liang (2010) conducted a survey on the IoT-based technologies. Different IoT application areas were discussed, including supply chain management, transportation, healthcare, disaster alerting and recovery. The authors mentioned some of the open issues associated with the IoT, such as standardization, security, privacy, and governance. It was concluded that the IoT success would depend on cooperative efforts in the relevant fields. Alam et al. (2011) pointed out that security and interoperability hinder the IoT-enabled service innovations. The study aimed to address the secure access issues for the IoT services and interoperability of security attributes among various business domains (e.g., railway operator vs. service provider). Each domain was assumed to be unique with its own security attributes and constraints. It was underlined that the integration of various administrative domains that rely on the IoT could be challenging due to different definitions of contents, contexts, and major roles.

Qi-cong (2011) discussed the inception, attributes, and classifications of the IoT-based technologies. The study provided a comparative analysis of different IoT functions. Furthermore, the main IoT applications in the military operations were explored, and the appropriate recommendations were provided. Shu et al. (2012) focused on the IoT applications in various rail transportation domains. The study specifically considered the interactions between three separate layers (the Ministry of Railways, the Railway Bureau, and the railway station site), aiming to understand the main business characteristics and information demand. A proper composition of the IoT technologies was found to be essential for the rail transportation development.

Zhang et al. (2017) discussed the Third Generation Partnership Project which relies on the deployment of 5G technologies and new radio interface. The main objective of the system is to provide a platform with different services for a variety of stakeholders (e.g., mission critical communications, automotive industry, railway industry). The study pointed out that the Vehicle-to-Everything (V2X) and IoT would be critical services for the new 5G system. Pirl (2019) indicated that the IoT systems are projected to grow in quantity and complexity in the following years. The concept of software fault injection (SFI) was evaluated for the dependability assessments. A case study was conducted for the wireless network standard IEEE 802.11p and vehicle-to-vehicle (V2V) communications. It was found that the latency of initiated communications was lower when comparing to conventional wireless networks. The study pointed out that the conducted work would be of relevance to manufacturing industries, railway companies, and major research organizations.

3.5. *Emerging communication technologies*

Several studies were dedicated to the next generation communication technologies that could be potentially applied in the railway industry and facilitate sustainable railway management and operations. Khutey et al. (2015) underlined the importance of advanced communication technologies. The study focused on the new generation technologies (i.e., 6G and 7G). The 6G technology was described as an integration of the 5G wireless mobile system and the satellite network which includes earth imaging satellite network, telecommunication satellite network, and navigation satellite network. The 7G technology would have similarities with the 6G but would also have specific satellite functions for mobile communication. It was concluded that the 6G and 7G communication technologies would change human lives. Spencer et al. (2017) proposed a wireless smart sensor (WSS) platform that could enable cost-effective, accurate, and fairly straightforward approach for structural health monitoring. The presented platform was found to be effective, as it could address structural health monitoring needs, overcome data loss challenges, enable synchronized sensing, and implement the required numerical algorithms.

Elmeadawy and Shubair (2019) provided a detailed review of the 6G wireless communication technology. It was pointed out that the 6G includes a wide range of features and attributes, including: terahertz communication, cell-free communication, artificial intelligence, holographic beamforming (HBF), extended reality, blockchain technology, and others. Furthermore, the study presented a detailed comparison between the 5G and 6G technologies (see Table 2). Akyildiz et al. (2020) studied advanced wireless communication systems with a primary focus on the 6G technology. Some of the major 6G goals were found to be: (1) maintain a terahertz-band operating network with a wide spectrum of resources; (2) support intelligent communication environments; (3) provide AI-based solutions; (4) enable full automation for large-scale networks; (5) dynamic spectrum access; (6) energy savings; (7) maintain the IoT efficiency; and (8) support MIMO communication networks. The terahertz band which lies between the mmWave spectrum and the infrared light spectrum (see Fig. 24) is expected to offer substantial spectrum resources for wireless communications. Deebak and Al-Turjman (2020) pointed out that the 6G technologies could improve the data transmission rates along with the system capacity for unmanned aerial vehicles (UAVs). The quality of experience could be substantially enhanced for different environments, including smart homes, parking,

Table 2
Comparison between the 5G and 6G technologies.

Characteristics	5G	6G
AI Integration	Partially	Fully
Automation Integration	Partially	Fully
Center of Gravity	User	Service
C-plane Latency	10 msec	1 msec
Downlink Data Rate	20 Gbps	1 Tbps
Extended Reality Integration	Partially	Fully
Haptic Communication Integration	Partially	Fully
Localization Precision	10 cm on 2D	1 cm on 3D
Maximum Mobility	500 km/h	1000 km/h
Operating Frequency	3–300 GHz	Up to 1 THz
Processing Delay	100 ns	10 ns
Reliability	10^{-5}	10^{-9}
Satellite Integration	No	Fully
Spectral Efficiency	10 bps/Hz/m^2	1000 bps/Hz/m^2
Time Buffer	Not Real Time	Real Time
Traffic Capacity	10 Mbps/m^2	1–10 Gbps/m^2
Uniform User Experience	50 Mbps 2D	10 Gbps 3D
U-plane Latency	0.5 msec	0.1 msec
Uplink Data Link	10 Gbps	1 Tbps

agriculture, and automation. It was concluded that the integration of UAVs and the satellite would address some of the major technological limitations.

Liu et al. (2020) indicated that the 6G would rely on data-driven machine learning (ML) which could be achieved by means of the AI techniques. Due to limitations of the traditional ML techniques, the study proposed federated learning to achieve ubiquitous AI in the 6G. Federated learning was defined as an emerging AI approach with privacy preservation that would be efficient for a wide range of different wireless applications. Shoewu and Ayangbekun Oluwafemi (2020) discussed the next generation mobile wireless networks with a primary emphasis on the 7G. Some of the major advantages of the next generation wireless networks were highlighted, including fast access to the internet, automation, energy efficiency, satellite-to-satellite communication, and sea-to-space communication. It was indicated that the 7G would be able to assist with effective health monitoring, air quality measurements, disaster preparedness, and treat detection. Malik et al. (2021) underlined that fog computing could be an effective technology for storage and computer services of the future 6G networks. However, the IoT technologies and fog nodes have certain energy limits which indicate the need for energy-efficient solutions. The study discussed various energy-efficient fog computing techniques that would be essential for the IoT and 6G (e.g., energy-aware task offloading, energy-aware device control, energy-aware fog node placement).

Mahmoud et al. (2021) conducted a detailed survey of applications, technologies, research problems, and challenges associated with the 6G. It was pointed out that the 6G technologies are expected to handle a large amount of data in smart cities with significantly lower latency. The following issues were found to be critical for the 6G: malicious behavior, unauthorized access control, data encryption, and data communication. Autonomous systems, connected robotics, wireless brain-computer interactions, blockchain, and distributed ledger technologies were identified as some of the major 6G applications. Yang et al. (2021) indicated that the traditional ML is centralized in data centers. However, there are growing concerns associated with the security of abundant data along with the computational resources for wireless communication networks. Such issues led to the development of federated learning with two major components, such as ML and wireless communications. The study discussed the main requirements for deploying federated learning in wireless communications. The conducted research could serve as a foundation for designing, optimizing, and operating federated learning-based wireless communication networks.

3.6. IoT challenges

Van Kranenburg and Bassi (2012) highlighted that the major IoT challenges cannot be managed with the existing research initiatives and policy tools, as these initiatives and tools are rather slow and too instrumental. The study outlined the following key IoT challenges: (1) new currencies and business models; (2) challenges in global cooperation; (3) control society, ethics, surveillance and data-driven life; and (4) technological issues that are caused by the necessity of saving energy. Privacy was indicated as one of the main ethical concerns that could be caused by the IoT-based applications. Song (2013) underlined that the IoT security should be strengthened to improve user experience. It was pointed out that the identity authentication and the traditional access control generally work in the same layer. The study suggested a security model addressing the IoT security issues. The proposed approach ensured enhanced privacy protection from the object application layer. Furthermore, the IoT object security access model was designed as well which allowed accessing the objects from different domains using just one sign-on.

Alrawais et al. (2017) proposed a technology of fog computing to overcome the gap between IoT devices and remote data centers. The expected advantages included: (1) improved security; (2) bandwidth reduction; and (3) decrease in latency. The fog computing technology is suitable for many IoT-enabled services. The security and privacy issues associated with the IoT applications were discussed in detail, including trust, authentication, access control, rogue node detection, intrusion detection, and data protection. The study also proposed a fog-based mechanism for security enhancement. Husamuddin and Qayyum (2017) discussed security threats involved in various IoT applications. A few of the major IoT application areas were presented: (1) environmental monitoring; (2) infrastructure management; (3) manufacturing; (4) home automation; (5) transportation; and (6) medical and healthcare system. Different security threats were discussed, including physical attacks, node replication, selective forwarding, wormhole attacks, sybil attacks, sinkhole attacks, and service denial attack. It was highlighted that user trust can be provided by deploying specific techniques for protecting data, privacy, and ethical practices.

Zeinab and Elmustafa (2017) discussed the concept of IoT, its applications and future technologies, and various challenges being faced in the implementation of the IoT technology. The study discussed some of the major IoT technologies, including sensing technologies (e.g., Wi-Fi, RFID, Bluetooth, and ZigBee) and connectivity-enabling technologies (e.

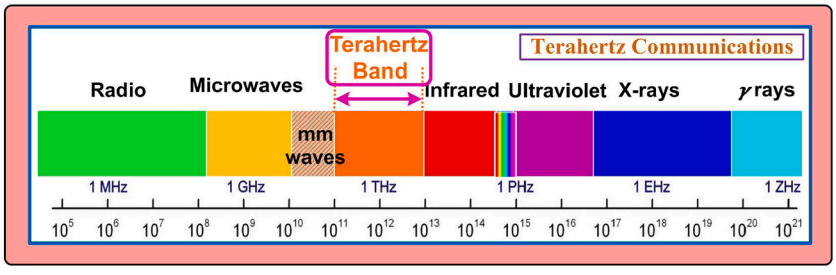


Fig. 24. Illustration of the Terahertz band.

g., 3G, GPRS, GSM, and LTE). It was pointed out that some of the large-scale IoT services are often vulnerable to disruptions as well as information theft. The appropriate mechanisms and techniques are required to ensure that some major services (e.g., city infrastructure, transport, energy) would not be disrupted as a result of security threats. Kumar et al. (2018) mentioned that the IoT altered the traditional lifestyle into a high-tech lifestyle. The IoT technologies facilitated the development of smart homes, smart cities, smart transportation, and smart industries. However, there are many different challenges that are associated with the IoT applications. The following issues were identified as the major IoT issues: (a) security and privacy; (b) interoperability/standard issues; (c) ethics, law and regulatory rights; (d) scalability, availability and reliability; and (e) quality of service. It was pointed out that the IoT developers should keep in mind these major issues and develop potential solutions to address them.

Leles et al. (2018) indicated that wireless network technologies are essential for the deployment of data communication systems in railway operations. However, wireless solutions for underground railways were identified to be a big challenge. The following challenges were found to be significant and could potentially impact railway networks: (1) environmental characteristics; (2) mobility; (3) independent frequency network; (4) bandwidth in wireless technology; (5) safety, availability, and network reliability; (6) quality of service; (7) open standards and cybersecurity; (8) big data and data management; (9) energy efficiency; and (10) virtualization. The study concluded that new intelligent technologies would be needed for the underground railway applications. Sharma et al. (2018) listed some of the key IoT elements, including WSN, RFID, near field communication (NFC), data storage and analytics, and data visualization. The study mentioned that the IoT-based technologies have been successful in many different applications, such as smart cities, smart homes, smart buildings, smart grid, smart energy, smart health, smart transportation, smart mobility, smart manufacturing, and smart factory. Despite various IoT advantages, some major challenges were highlighted in the study as well (e.g., scalability, self-organization for specific environments, data volumes, data interpretation, interoperability, power supply, wireless communications, security and privacy). Ongoing technological developments are expected to overcome the IoT challenges in the following years and better satisfy user needs.

Virat et al. (2018) discussed experimental drawbacks associated with 3-layered and 4-layered architectures in the IoT technology applications. A 5-layered architecture was proposed to overcome the existing drawbacks. The developed 5-layered architecture included the following elements: (a) perception layer which identifies and digitalizes the sensor data; (b) network layer which ensures connectivity and secured communication with the IoT devices; (c) processing layer which is responsible for interoperability, data storage, and data retrieval; (d) application layer which enables global management and services; and (e) business layer which presents the results collected from other layers. The study also discussed the IoT issues associated with privacy and security. Dabbagh and Rayes (2019) specifically focused on the IoT challenges related to privacy and security. It was indicated that the privacy and security issues could significantly disrupt human lives if not addressed properly. The damages caused by cyber-attacks could potentially affect physical objects that are used in everyday life. Furthermore, the IoT security risks can be damaging to business enterprises (e.g., an attacker hacks the system and is able to spy on the company). A variety of countermeasures were discussed that could address privacy and security challenges, such as limiting cache switching rate, hard isolation, encrypting migrated memory pages, server authentication, adding an isolation domain between the hardware and hypervisor, and secret storage via data chopping.

Polat and Sodah (2019) also studied the security issues that can be caused by the IoT applications. The most common weaknesses of the IoT applications were found to be insufficient authentication, insecure web interface, lack of appropriate encryption, insecure network services, insecure mobile interface, insecure cloud interface, and insecure software. The study proposed several countermeasures, including the following: (1) multiple layers of technical, administrative, and physical controls; (2) security should be an integral part of manufacturing; (3) embed firewall features to address cyber-attacks; (4) thorough testing of the IoT devices for security issues; (5) segmentation of the IoT devices (e.g., unused services can be closed/deactivated); (6) improve authentication, so only trusted devices could exchange the data); and (7) user awareness trainings. SNCF et al. (2020) provided recommendations in order to protect the IoT applications against cyber-attacks in the railway industry. It was indicated that security should be ensured throughout the entire IoRT lifecycle, including provisioning, deployment, operation, update, and decommission. The study also presented a vision for the next generation railway cybersecurity. It was underlined that the increasing machine-to-machine communication will eliminate human intervention which demands careful security supervision for detecting cyber-attacks and misuse.

Abosata et al. (2021) conducted a detailed survey covering the issues of security, attacks, and potential countermeasures that could be used in the IIoT applications. The study discussed the security issues related to the perception layer, network layer, and application layer and presented a variety of countermeasures that could be adopted for each layer (see Fig. 25). It was pointed out that specific countermeasures need further developments for cyber-attacks in particular IIoT environments, such as transportation, smart grid, and smart industry. Novel intrusion detection technologies are required to protect provided services and connected systems. Zikria et al. (2021) discussed various opportunities, challenges, and solutions for the next generation IoT technologies. Some of the domains with a wide implementation of the IoT technologies were identified to be smart healthcare, smart cities, smart agriculture, data analytics, IIoT, multimedia, and spectrum sharing techniques. The authors indicated that the security and privacy challenges are viewed as one of the main barriers towards full perception of the IoT-based technologies. Furthermore, the AI-based IoT devices encounter many challenges due to high user density, low power of devices, data loss, and high latency.

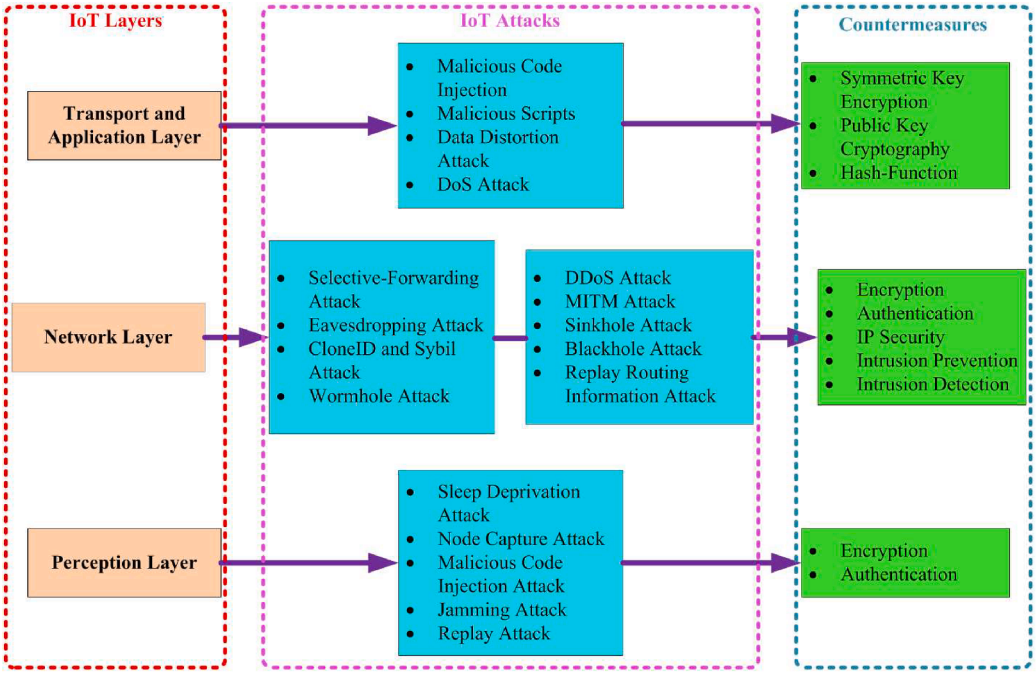
4. State-of-the-Art summary

Table 3 provides a concise summary of the relevant state-of-the-art efforts and presents the following elements for each one of the reviewed studies: (1) author(s) and year; (2) study objective; and (3) notes, important considerations, and study outcomes.

4.1. Key advantages of the IoT applications

A detailed survey of the relevant state-of-the-art efforts revealed the following major advantages of the IoT applications for railway transportation systems:

- The IoT applications enable ***effective management of railway operations*** (Li et al., 2014). The IoT-based technologies are capable to forecast the demand for rail transportation services which can be further used to allocate the available resources accordingly. Moreover, the IoT devices assist with effective information perception, sharing, real-time sensing, intelligent analysis, train tracking and positioning, automatic fare collection, security early warning, station train information sharing, cargo management, and warehouse management (Zhang et al., 2011; Lei et al., 2013; Shi and Wang, 2013). All the aforementioned activities are essential for proper railway operations scheduling and management.
- Various IoT technologies have been successfully used for ***monitoring, maintenance, and repair of railway segments*** (Zhang, 2012; Chapman et al., 2016; Karaduman et al., 2018; Shankar et al., 2019; Mohamed et al., 2020). The IoT applications are able to identify defective rail segments in real time and transmit safety alerts to the appropriate personnel when needed. A timely response to safety



Notes: DoS Attack – Denial-of-Service Attack; DDoS Attack – Distributed Denial-of-Service Attack; MITM Attack – Man-in-the-Middle Attack; IP Security – Internet Protocol Security.

Fig. 25. Classification of IoT layers, potential attacks, and countermeasures.

issues is critical to ensure continuity of services for passenger and freight trains.

- The IoT-based technologies may assist with ***proper maintenance of trains*** throughout the entire life cycle (Zhang, 2012; Zhong et al., 2021). The relevant data can be collected from trains, processed, and submitted to the appropriate personnel. The appropriate personnel can schedule necessary maintenance activities accordingly to prevent potential breakdowns of passenger and freight trains.
- The IoT applications may ***enhance rail transportation safety*** by preventing freight theft issues, reducing fire hazards, and ensuring proper maintenance monitoring and inventory management (Ling, 2013; Zhang and Shao, 2013). An enhanced safety level is one of the critical factors that could improve competitiveness of rail transportation compared to other transportation modes.
- The IoT may assist the railway operators ***improving the level of service and passenger comfort*** (Gangwar et al., 2017; Ganga et al., 2019). The IoT devices can be used to assign certain tasks to the available crew members to make sure that the passenger requests will be addressed in a timely manner. Furthermore, passenger requests could be prioritized by the IoT-enabled technologies in an intelligent manner (e.g., emergency requests should receive a higher priority when comparing to dining service requests).
- The IoT-based technologies will be able to assist with ***meeting sustainable development goals*** (Adebiyi and Cruz, 2018). The sustainable development goals can be achieved by improved management, decarbonization, reduced energy consumption, and better utilization of the available assets. Green IoT technologies are expected to overcome the limitations of the existing technologies in terms of emissions, energy waste, excessive use of fuel, and greenhouse effects (Solanki and Nayyar, 2019).
- The IoT can enhance the performance of ***maglev rail transit systems*** (Kumar et al., 2020; Sun et al., 2020). The IoT-based technologies ensure effective monitoring of maglev trains and improve the safety of trains and passengers. Advanced control algorithms along with modern communication technologies are generally used to monitor the status of the magnetic suspension system and ensure proper operations of maglev trains.
- The IoT applications are expected to facilitate ***automation of rail transportation services***. The IoT technologies would allow achieving all the benefits from automation without affecting safety in a negative way (Castillo, 2019). Advanced sensors, cloud computing, and predictive data analytics are some of the key IoT features that would promote further development of autonomous rail transportation systems.
- Deployment of the AI-based solutions may address ***a variety of railway operational issues*** that include, but are not limited, to maintainability, reliability, security, safety, and performance (Flammini et al., 2020). The AI algorithms are able to monitor railway operations in real time, detect potential cyber-threats, and block cyber-threats to prevent malfunctioning of relevant software and equipment. Moreover, the AI can effectively solve challenging decision problems associated with railway operations (e.g., timetabling, real-time rescheduling of the available resources) in a timely manner.

4.2. *Key challenges associated with the IoT applications*

Along with a variety of advantages from the deployment of IoT applications, many challenges have been discovered throughout the present survey as well. These challenges must be addressed by relevant stakeholders to assure sustainable development and deployment of the IoT applications in railway transportation systems and other domains. The identified challenges were further categorized in the following groups: (1) technological challenges; (2) operational challenges; (3) privacy and security challenges; (4) standardization and legal challenges; and (5) other challenges.

4.2.1. *Technological challenges*

- **Heterogeneity**: Many heterogeneous IoT technologies have been actively used in various domains. Different environments and applications may require different networking capabilities and technologies as well as other characteristics (e.g., cellular network, wireless local area network, RFID technologies) that substantially

Table 3
Summary of the relevant state-of-the-art efforts.

a/a	Author(s) and Year	Study Objective	Notes, Important Considerations, and Study Outcomes
IoT Applications for Sustainable Railway Management and Operations			
1	Liu et al. (2010)	Explore potential advantages of using the IoT in the railway industry.	The study proposed a real-time tracking application that could be used to monitor the state of the goods throughout transportation by rail. The developed method attempted to facilitate docking between the rail and road modes.
2	Zhang et al. (2011)	Study the IoT deployment for the Chinese railway system.	The IoT-based technologies could assist with a variety of operations, including train tracking and positioning, automatic fare collection, security early warning, station train information sharing, cargo management, and warehouse management.
3	Zhang (2012)	Study the deployment of various IoT technologies for high-speed trains.	The IoT could be used to identify defects of trains in real time and transmit safety alerts when needed. The study underlined that the IoT could improve maintenance efficiency, reduce labor intensity and failure likelihood.
4	Lei et al. (2013)	Improve the existing railway transportation services in China.	The study proposed an IoT-based framework which included a perceptual recognition layer, access layer, carrying network layer, application controlling layer, and intelligent application layer.
5	Ling (2013)	Improve rail transportation safety.	Application of intelligent IoT devices would prevent freight theft issues, reduce fire hazards, ensure proper maintenance monitoring and inventory management, as well as improve economic benefits of safety.
6	Shi and Wang (2013)	Enhance the flow of railway information.	An intelligent railway information platform was established which relied on the basic environmental layer, integrated IoT application layer, application support layer, and railway transportation application layer.
7	Zhang and Shao (2013)	Develop an IoT-based architecture for railway safety monitoring in China.	Despite substantial IoT advantages for railway safety monitoring, it may take a significant amount of time before the IoT technologies would be heavily deployed on railway segments.
8	Li et al. (2014)	Assess challenges of the Beijing rail transit network (China).	The study proposed an IoT-based system for mass passenger rail transit that relied on information sharing, real-time sensing, and intelligent analysis.
9	Ai et al. (2015)	Develop a wireless communication network for rail transportation.	The suggested methodology is anticipated to meet the requirement of high spectrum and high-data-rate efficiency.
10	Eiza et al. (2015)	Develop the "RIoT" (Rail Internet of Things).	The study outlined potential security risks for the RIoT and proposed certain countermeasures (e.g., encryption of communication channels, risk analysis for the available devices).
11	Chapman et al. (2016)	Propose an emerging IoT-based technology.	The suggested IoT technology enabled high-resolution cost-effective rail moisture monitoring.
12	Gangwar et al. (2017)	Design a new IoT-based system for passenger service.	A multi-objective optimization algorithm was developed to allocate the available crew members for service of passengers, considering the information regarding location, service arrival time, and workload factor.
13	Jo et al. (2017)	Present a low-cost IoT solution for smart railway infrastructure.	It was found that the developed IoT-based solution was able to easily handle the condition information for the railway infrastructure.
14	Li et al. (2017)	Development of smart railway technologies.	The authors presented the architecture for smart railways that included a total of four layers: (a) perception and action layer; (b) transfer layer; (c) data engine layer; and (d) application layer.
15	Zheng et al. (2017)	Protect confidentiality and integrity of the information.	The conducted analysis demonstrated that the developed method was able to guarantee an appropriate security level in railway operations.
16	Karaduman et al. (2018)	IoT-based condition monitoring of railway operations.	The proposed methodology relied on cameras that were monitoring dedicated railway segments and taking images which were further transmitted to a central computer.
17	Naser (2018)	Study the blockchain applications related to the railway industry.	It was pointed out that the blockchain applications had only a moderate adoption rate in the railway industry which does not allow full exploration of their benefits.
18	Saghafi and Kordsalari (2018)	Facilitate the IoT deployment on the Iranian railways.	A number of challenges in the IoT deployment were identified (e.g., old infrastructure, equipment theft, resistance to change, sanctions, conflict of interest for certain stakeholders,

(*continued on next page*)

Table 3 (*continued*)

a/a	Author(s) and Year	Study Objective	Notes, Important Considerations, and Study Outcomes
			technological illiteracy, cost, moral indifference).
19	Sneps-Sneppe and Namiot (2018)	Ensure reliable connectivity for efficient, safe, and attractive railway services.	The Moscow urban railway project was considered as a practical example. It was indicated that high-speed railway services were needed to support physically separated territories.
20	Castillo (2019)	Study automation in rail transportation.	It was indicated that the IoT technologies would allow achieving all the benefits from automation without affecting safety in a negative way.
21	Ganga et al. (2019)	Develop an IoT-based methodology for passenger rail services.	The requests from passengers (e.g., medical services, blanket services, catering services, emergency issues) were allocated among the available crew members based on the established priority schedule.
22	Shankar et al. (2019)	Detection of cracks in rail tracks and major landslides in hilled areas.	The proposed system could detect the existing hazards and transmit the information to the nearest station.
23	Xie and Qin (2019)	Perimeter intrusion detection at high-speed railways.	A custom data-fusion algorithm was presented to process the data collected from multiple sensors and improve the detection accuracy.
24	Ai et al. (2020)	Improve high-speed railway operations.	A network slicing architecture was proposed for the 5G high-speed railway system. Based on the conducted experiments, significant 5G-based key technologies were identified.
25	Arunjyothi and Harikrishna (2020)	Enhance the performance of radio access technologies.	The authors introduced a new network architecture to improve the efficiency of radio access technologies in the railway field conditions.
26	Dirnfeld et al. (2020)	Investigate the LPWAN potential for smart railways.	Both IoT and LPWAN would be very promising technologies for cost-effective remote monitoring, surveillance, and control over large geographical areas even in case of situations where the power supply is restricted.
27	Flammini et al. (2020)	Analyze the prospects of integrating the AI in railway operations.	The AI technologies would be efficient in addressing certification issues and emerging threats.
28	Mohamed et al. (2020)	Develop an integrated maintenance logistics monitoring system for high-speed rail.	The results from the conducted experiments indicated that the proposed system could be effective to ensure adequate maintenance activities and assist with a timely response to urgent repair orders.
29	Sun et al. (2020)	Study the use of IoT technologies in maglev rail transit systems.	The research suggested an IoT-based adaptive fuzzy controller for supervising medium to low-speed maglev trains.
	IoT Applications at Level Crossings		
30	Dhande and Pacharaney (2017)	Study level crossing safety at unmanned crossings.	The study proposed an IoT-based system which included sensors, Global Positioning System (GPS), and Global System for Mobile Communication (GSM).
31	Minoli and Occhiogrosso (2017)	Address rail track intrusions at level crossings.	The study proposed an IoT-based approach for sending alerts due to static and dynamic rail track intrusions at level crossings.
32	Virtanen et al. (2019)	Investigate the safety challenges of autonomous vehicles approaching level crossings.	It was pointed out that the perception sensors of autonomous vehicles, vehicle-to-everything messaging, and train-tracking solutions could facilitate safe passage of vehicles through level crossings.
33	Aziz et al. (2020)	Detection of the objects on the railway tracks and their vicinity.	The IoT system was used for monitoring and storing the data regarding the objects in the vicinity of rail tracks. The radar and processing software were used to display the distance between the objects and the device.
34	Ranjith and Vijayaragavan (2020)	Study level crossings safety in Tanzania.	The study proposed the IoT-based mechanisms that can operate automatically without any human involvement.
35	Singh et al. (2020)	Develop an automated vehicle detection system.	The proposed vehicle detection system is likely to enhance traffic control at level crossings and decrease the number of accidents.
36	Prasad and Madhumathy (2021)	Design a new IoT-based system for railway maintenance.	The IoT system could prevent major accidents or alleviate the associated effects in case of the accident occurrence (e.g., train derailment in the vicinity of level crossings).
37	Talpur et al. (2021)	Investigate gate opening and closing operations at level crossings.	The study proposed force-sensitive resistor detectors for automatic side road crossing protection. The proposed system could directly communicate with the nearest control room in case of unexpected situations.
38	Singh et al. (2021a)	Study current trends in the deployment of autonomous trains.	It was indicated that advanced IoT technologies (e.g., DSRC technologies) would prevent potential conflicts between autonomous vehicles and autonomous trains which would further increase safety of users at level crossings.

(*continued on next page*)

Table 3 (*continued*)

a/a	Author(s) and Year	Study Objective	Notes, Important Considerations, and Study Outcomes
Green IoT Applications			
39	Fraga-Lamas et al. (2017)	Investigate potential advantages of the commercial IIoT for the railway industry.	The study pointed out that emission reduction could be achieved by optimizing train timetables, use of energy storage devices, smart metering methods, and optimized train trajectories.
40	Adebiyi and Cruz (2018)	Evaluate the existing IoT-based green sustainability technologies for the railway industry in Malaysia.	Additional considerations should be given to adequately address the green and sustainable development goals (e.g., improved management, decarbonization, reduced energy consumption, better utilization of the available assets).
41	Elmustafa and Mujtaba (2019)	Propose the concept of "smart environment".	The IoT could assist with sensing, monitoring, and tracking the objects of environment which can further facilitate green and sustainable lifestyle.
42	Perwej et al. (2019)	Review the IoT applications in different domains.	It was indicated that the IoT applications could be effectively used to measure the emission levels in different parts of the city (e.g., metro stations, crowded areas, parks, etc.).
43	Solanki and Nayyar (2019)	Investigate the implementation of green IoT (G-IoT) in different domains.	The G-IoT applications are expected to overcome the limitations of the existing technologies in terms of emissions, energy waste, excessive use of fuel, and greenhouse effects.
44	Zantalis et al. (2019)	Evaluate the ML and IoT applications in smart transportation systems.	The study pointed out that ML and IoT could assist with route optimization. Optimized transportation routes are expected to minimize traffic congestion at busy roadway and rail corridors and decrease the associated emissions produced by vehicles.
45	Mehmood et al. (2021)	Study the integration of smart grid, IoT, and edge computing.	Smart grid can provide green and renewable energy solutions for smart cities (including smart transportation systems), and its efficiency can be substantially augmented with the new technologies (i.e., IoT, edge computing, big data, and artificial intelligence).
46	Zhong et al. (2021)	Investigate the key IoT technologies for high-speed railway systems.	It was concluded that the IoT deployment could improve environmental sustainability of high-speed railway systems, along with enhanced safety, efficiency, and comfort.
General Studies on the IoT Technologies and Applications			
47	Sundmaeker et al. (2010)	Review the current IoT deployment efforts in various countries.	The study described the Cluster of European Research Projects on the Internet of Things which included a total of 30 major research initiatives in the field of advanced technologies (e.g., sensing technologies, detection technologies).
48	Economides (2016)	Study user perception towards the IoT technologies.	The research suggested an IoT-based model to address user perception towards the IoT technologies. The proposed model directly considered user characteristics (e.g., age, gender, education, and experience with computers).
49	Bali et al. (2018)	Describe different applications of the IoT.	It was pointed out that the external environmental factors (e.g., temperature) could significantly influence the IoT services.
50	Chapman and Bell (2018)	Investigate the IoT applications for monitoring infrastructure.	It was underlined that low-cost IoT sensors showcase adequate performance. However, age of the technology could affect the accuracy of collected data. Another challenge was found to be annual calibration and maintenance.
51	Bansal and Lal (2019)	Study the IoT technologies and applications.	The study mentioned that the IoT could improve quality of life, as many devices could be automated and more efficient energy utilization might be achieved.
52	Gharami et al. (2019)	Investigate different approaches being used by the IoT.	The study specifically indicated that one of the main obstacles behind the broad IoT implementation is the lack of compatible devices along with the security and privacy issues.
53	Chen (2020)	Explore the concept of "the Internet of Video Things (IoVT)."	A self-learning capability was found to be the major feature that would be essential for the future IoVT technologies.
54	Adil and Khan (2021)	Review of the Healthcare IoT (H-IoT) applications.	It was indicated that the H-IoT systems are complex and are represented not only by cluster heads, sensors, controls, and base stations but also by humans (nurses, patients, and pharmacists).
55	Mehmood et al. (2021)	Investigate new technologies for smart grid.	The study proposed to use the edge computing technologies for the IoT smart grid to address the security, latency, privacy, and high bandwidth utilization issues.
56	Pal et al. (2021)	Study the blockchain solutions for the IoT access control.	Several blockchain attributes, such as secure storage, decentralized control, and information sharing, were found to be

(*continued on next page*)

Table 3 (*continued*)

a/a	Author(s) and Year	Study Objective	Notes, Important Considerations, and Study Outcomes
			essential for the IoT access control.
57	Wang and Sarkis (2021)	Describe the trends in digitalization of freight transportation.	Some of the major technologies were discussed to show how these technologies could create significant changes in supply chains and logistics systems.
58	Yi and Liang (2010)	Survey the IoT-based technologies.	Different IoT application areas were discussed, including supply chain management, transportation, healthcare, disaster alerting and recovery.
59	Alam et al. (2011)	Discuss the secure access issues for the IoT services.	The study aimed to address the secure access issues for the IoT services and interoperability of security attributes among various business domains.
60	Qi-cong (2011)	Review the inception, attributes, and classifications of the IoT-based technologies.	The study provided a comparative analysis of different IoT functions. Furthermore, the main IoT applications in the military operations were explored, and the appropriate recommendations were provided.
61	Shu et al. (2012)	Investigate the IoT applications in various rail transportation domains.	The study specifically considered the interactions between three separate layers (the Ministry of Railways, the Railway Bureau, and the railway station site), aiming to understand the main business characteristics and information demand.
62	Zhang et al. (2017)	Discuss the Third Generation Partnership Project.	The main objective is to provide a platform with different services for a variety of stakeholders (e.g., critical communications, automotive industry, railway industry).
63	Pirl (2019)	Evaluate the software fault injection concept.	It was found that the latency of initiated communications was lower when comparing to conventional wireless networks.
Emerging Communication Technologies			
64	Khutey et al. (2015)	Survey the new generation technologies (i.e., 6G and 7G).	The 7G technology would have similarities with the 6G but would also have specific satellite functions for mobile communication.
65	Spencer et al. (2017)	Develop a wireless smart sensor platform.	The presented platform was found to be effective, as it could address structural health monitoring needs, overcome data loss challenges, enable synchronized sensing, and implement the required numerical algorithms.
66	Elmeadawy and Shubair (2019)	Review the 6G wireless communication technology.	It was pointed out that the 6G includes a wide range of features and attributes, including: terahertz communication, cell-free communication, artificial intelligence, holographic beamforming (HBF), extended reality, and blockchain technology.
67	Akyildiz et al. (2020)	Study advanced wireless communication systems.	The terahertz band is expected to offer substantial spectrum resources for wireless communications.
68	Deebak and Al-Turjman (2020)	Deployment of the 6G technologies for drones.	The 6G technologies could improve the data transmission rates along with the system capacity for unmanned aerial vehicles (UAVs).
69	Liu et al. (2020)	Explore the potential of federated learning.	Federated learning was described as an emerging AI approach that would be efficient for a wide range of different wireless applications.
70	Shoewu and Ayangbekun Oluwafemi (2020)	Discuss the next generation mobile wireless networks with a primary emphasis on the 7G.	Some of the major advantages of the next generation wireless networks were highlighted, including fast access to the internet, automation, energy efficiency, satellite-to-satellite communication, and sea-to-space communication.
71	Malik et al. (2021)	Review of the fog computing technologies for the 6G.	The study discussed various energy-efficient fog computing techniques that would be essential for the IoT and 6G (e.g., energy-aware task offloading, energy-aware fog node placement, energy-aware device control).
72	Mahmoud et al. (2021)	Review of the 6G applications.	Autonomous systems, connected robotics, wireless brain-computer interactions, blockchain, and distributed ledger technologies were identified as some of the major 6G applications.
73	Yang et al. (2021)	Study the main requirements for deploying federated learning.	The conducted research could serve as a foundation for designing, optimizing, and operating federated learning-based wireless communication networks.
IoT Challenges			
74	Van Kranenburg and Bassi (2012)	Investigate the IoT challenges.	The major IoT challenges cannot be managed with the existing research initiatives and policy tools, as these initiatives and tools are rather slow and too instrumental.
75	Song (2013)	Study the IoT security.	The study suggested a security model addressing the IoT security issues.

(*continued on next page*)

Table 3 (*continued*)

a/a	Author(s) and Year	Study Objective	Notes, Important Considerations, and Study Outcomes
			The proposed approach ensured enhanced privacy protection from the object application layer.
76	Alrawais et al. (2017)	Analyze the security and privacy issues for the fog computing technology.	The security and privacy issues associated with the IoT applications were discussed in detail, including authentication, trust, rogue node detection, access control, intrusion detection, and data protection.
77	Husamuddin and Qayyum (2017)	Investigate the IoT security and privacy threats.	Different security threats were discussed, including physical attacks, node replication, selective forwarding, wormhole attacks, sybil attacks, sinkhole attacks, and service denial attack.
78	Zeinab and Elmustafa (2017)	Review the IoT applications and challenges.	It was pointed out that some of the large-scale IoT services are often vulnerable to disruptions as well as information theft.
79	Kumar et al. (2018)	Survey the IoT technologies and implementation challenges.	The following issues were identified as the major IoT issues: (a) security and privacy; (b) interoperability/standard issues; (c) ethics, law and regulatory rights; (d) scalability, availability and reliability; and (e) quality of service.
80	Leles et al. (2018)	Study the IoT challenges for wireless communications.	Wireless solutions for underground railways were identified to be a big challenge. The study concluded that new intelligent technologies would be needed for the underground railway applications.
81	Sharma et al. (2018)	Investigate the IoT applications and challenges.	Some major challenges were highlighted in the study (e.g., scalability, self-organization for specific environments, data volumes, data interpretation, interoperability, power supply, wireless communications, security and privacy).
82	Virat et al. (2018)	Develop a 5-layered IoT architecture.	A 5-layered architecture was proposed to overcome the existing drawbacks of 3- and 4-layered architectures. The IoT issues associated with privacy and security were discussed as well.
83	Dabbagh and Rayes (2019)	Investigate the IoT security and privacy issues.	It was indicated that the privacy and security issues could significantly disrupt human lives if not addressed properly. The damages caused by cyber-attacks could potentially affect physical objects that are used in everyday life.
84	Polat and Sodah (2019)	Study the IoT security issues and potential countermeasures.	The most common weaknesses of the IoT applications were found to be insufficient authentication, insecure web interface, lack of appropriate encryption, insecure network services, insecure mobile interface, and insecure software.
85	SNCF et al. (2020)	Review the IoT security issues in rail applications.	It was underlined that the increasing machine-to-machine communication will eliminate human intervention which demands careful security supervision for detecting cyber-attacks and misuse.
86	Abosata et al. (2021)	Investigate the IoT security issues and potential countermeasures.	The study discussed the security issues related to the perception layer, network layer, and application layer and presented a variety of countermeasures that could be adopted for each layer.
87	Zikria et al. (2021)	Survey the next generation IoT opportunities and challenges.	The authors indicated that the security and privacy challenges are viewed as one of the main barriers towards full perception of the IoT-based technologies.

vary from one IoT application to another (Chen et al., 2014a; Ali et al., 2015). Furthermore, different IoT devices generally have different security countermeasures. New alternatives should be developed to effectively deal with heterogeneous IoT devices in a holistic manner.

- **Technology cost**: The available IoT communication technologies, including mobile and fixed communication systems, wireless communications, power line communications, and technologies for short-range wireless communication, should have an adequate cost (Chen et al., 2014a). High costs may negatively affect the IoT adoption rates across various sectors.
- **Reliable connectivity**: The available IoT communication technologies may significantly vary in terms of degree of their complexity. However, irrespectively of technology complexity, reliable connectivity of the IoT devices should be ensured for their successful implementation (Chen et al., 2014a).
- **Appropriate architecture**: The number of different IoT devices has been drastically increasing. The IoT services become more decentralized, mobile, and complex. The IoT systems are required to handle large volumes of data from different sources and support decision making. Therefore, one IoT architecture that is appropriate for a given domain may not be suitable for another domain (Gubbi et al., 2013; Chen et al., 2014a; Sarkar et al., 2015). Moreover, heterogeneous nature of protocols and standards for the existing IoT services and products imposes additional challenges in the architecture design (Bellavista et al., 2013; Udoh and Kotonya, 2018).
- **Hardware requirements**: The hardware requirements may significantly vary for different types of IoT terminals due to the differences in bandwidth (e.g., sensing a simple value vs. transmitting a video stream). Achieving low power consumption in a sleep mode and low cost is viewed as major issue that should be addressed by hardware developers (Chen et al., 2014a).

- **Stakeholder involvement**: The development of IoT-based technologies requires involvement of different stakeholders, including software designers, domain experts, device developers, application developers, and network managers. The stakeholders generally have their own policies and expectations (Udoh and Kotonya, 2018). However, all the stakeholders involved should collaboratively address the issues associated with the IoT application design, deployment, and evolution. Therefore, new collaborative mechanisms are needed to facilitate interactions between different stakeholders.

4.2.2. Operational challenges

- **Scalability**: Scalability aims to manage the sustainable growth of the IoT technologies in an efficient way and is one of the key challenges in the IoT implementation. Connecting the growing number of the IoT devices is viewed as a challenging task (Ali et al., 2015; Chen et al., 2014b). The devices are more likely to be arranged in hierarchical sub-domains rather than in a mesh (Van Kranenburg and Bassi, 2012). New alternatives should be developed in the future to ensure effective scalability in the IoT domains.
- **Interoperability**: Various IoT-based technologies with distinct characteristics are used by different industries. Interoperability between layers of these technologies is essential (e.g., physical layers, communication layers, functional layers, and application layers). The separate layers are generally developed using various protocols and languages. Innovative holistic approaches are necessary in order to support the interoperability of IoT-based technologies and services for each layer (Chen et al., 2014a; Ali et al., 2015; Udoh and Kotonya, 2018). In the meantime, low interference should be maintained for the IoT-devices that are intended to work separately (Chen et al., 2014b).
- **Networking**: Managing the IoT networks could be challenging. The information flow and protocols could influence the network behavior (Ali et al., 2015). In many instances, it is quite difficult to predict where a given IoT object should be moved, and the object may have to be shifted to a completely different network. Moreover, changes in dynamic gateways create challenges in identifying the exact locations of the IoT objects.
- **Routing**: Routing in the communication domain refers to the identification of the best possible path between the source and the destination with the overall objective of completing the communication process (Ali et al., 2015). There are different ways that can be used to select the best possible path, considering communication protocol type, cost, and bandwidth. New types of optimization algorithms are still needed to optimize routing of the IoT components and achieve energy savings.
- **Adaptability**: The IoT systems are composed of many nodes that are resource-constrained. In case of power shortage and/or poor connectivity, some nodes can be disconnected from the main system during certain time periods (Udoh and Kotonya, 2018). Moreover, the location, state, and computing speed of the existing nodes may change. All the aforementioned factors make the environment surrounding the IoT systems dynamic. Therefore, the IoT systems should be self-adaptive, self-optimizing, self-configuring, and self-protecting to ensure that planned services are provided under changing environmental settings.
- **Virtualization**: Virtualization refers to the ability of sharing the available hardware resources amongst multiple operating systems. The virtualization concept enables several operating systems and applications running on the same server (Ali et al., 2015). There are three common areas for virtualization, including server virtualization, storage virtualization, and network virtualization. The future IoT technologies should rely more on the virtualization concept, as it is expected to significantly increase the network performance, maximize scalability, enhance system utilization, and yield cost savings.
- **Operations in remote locations**: Operations of the IoT devices from remote locations are challenging due to the deployment of different sensors, roadside units at unmanned locations in various distant locations, such as highways, railways, and smart grid (Dabbagh and Rayes, 2019). The safety and security of these unmanned devices and sensors working either autonomously or remotely controlled can be compromised by unauthorized users. Therefore, additional monitoring systems (cyber and physical) should be installed at remote locations to ensure proper operations of the IoT applications.
- **Big data processing**: The IoT-based applications often have to deal with large volumes of data. Big data are common not only for the industrial applications but for various social networks as well. Traditional databases and software techniques will not be effective for storing and processing big data (Ali et al., 2015; Udoh and Kotonya, 2018; Aslam et al., 2020). New types of algorithms, including learning, adaptive, and self-adaptive algorithms (Kavoosi et al. 2019, 2020a; Dulebenets, 2021), should be developed in the following years in order to effectively handle large volumes of data and ensure proper functionality of the relevant IoT technologies. Furthermore, new data mining techniques should be developed for processing video data and unstructured images (Lee and Lee, 2015).
- **Application maintenance**: The growing number of IoT devices and applications will be distributed over a large network area. These applications will interact with each other in various complex ways. Since the IoT applications will serve large geographical locations with constantly changing environments, there is a need for effective maintenance (Udoh and Kotonya, 2018). The codes and programs that are used by the IoT applications should be regularly updated and debugged to ensure that the desired IoT services will be provided to the designated users. There are also challenges associated with remote maintenance, as remote debugging of applications may cause security and privacy concerns.
- **Power consumption**: Global IoT terminals, global IoT access points, global IoT access gateways, IoT data processing, and IoT infrastructures are expected to be some of the major power consumers across the globe in the following years (Chen et al., 2014a; Lanzisera et al., 2014; Rehman et al., 2017). The efficiency of the IoT sensors is typically affected with the battery lifetime (Ali et al., 2015). Hence, the development of new energy sources for the IoT devices (e.g., fuel cells, efficient batteries, new energy devices, new energy harvesting methods) are essential for the future autonomous wireless systems.
- **Quality of service**: The quality of service is typically defined as the amount of time that is required to deliver a message from the sender to the designated recipient (Ali et al., 2015). The quality of service is considered as satisfactory if the delivery time is less or equal to the pre-determined time which is established based on the customer preferences. The future IoT technologies and applications should be designed and implemented considering the quality of service requirements to ensure that the customer needs are effectively met.
- **Real-time response**: Certain IoT domains require services that are time-sensitive (e.g., healthcare, telemedicine, disaster response, vehicle-to-vehicle communication). Failure to provide a timely response may inevitably lead to negative externalities (e.g., loss of human lives in case of slow emergency response). Hence, the future IoT technologies serving time-critical domains should be designed and operated accordingly to ensure timely delivery of services and data (Udoh and Kotonya, 2018).

4.2.3. Privacy and security challenges

- **Security architecture**: The IoT-based systems will require unique security architecture (Chen et al., 2014a). The existing security architectures that are designed for human communications may not be

suitable for the IoT applications and negatively impact the functionality of the IoT technologies.

- **Security considerations in the IoT design**: Security is considered as a critical attribute of every IoT technology. Security considerations should be taken into account at the design and manufacturing stages, as they directly influence the major properties of hardware and software (Polat and Sodah, 2019). Furthermore, each IoT device should undergo a thorough testing before appearing on the market to ensure adequate response to various types of cyber-attacks.
- **Data confidentiality and integrity**: Data confidentiality ensures that only authorized users are allowed to access certain data and make the required alterations if needed. Data confidentiality is generally associated with two processes (Ali et al., 2015): (a) access control; and (b) object authentication. Maintaining data confidentiality is viewed as essential for the future development of the IoT-based technologies. Moreover, the IoT applications should meet the information integrity requirements, where the exchanged messages cannot be altered by any unauthorized party (Dabbagh and Rayes, 2019).
- **Secrecy**: There are two types of secrecy in the IoT systems (Dabbagh and Rayes, 2019): (a) forward secrecy; and (b) backward secrecy. The forward secrecy assures that when a given object leaves the IoT network, it will not have any access to the information after its departure. On the other hand, the backward secrecy assures that when a given object enters the IoT network, it will not have any access to the information before its entry. The future IoT applications should satisfy both forward and backward secrecy requirements.
- **Threat detection**: Effective treat detection remains one of the main challenges for the IoT systems (Roman et al., 2013; Wazid et al., 2016; Dabbagh and Rayes, 2019). New types of algorithms have to be developed to effectively identify potential threats that can disrupt the performance of IoT applications. Adaptive learning algorithms would be able to capture malicious attacks based on the features of the existing and already-known threats (Ray et al., 2014).
- **Authentication**: Authentication allows IoT users and devices to communicate and ensure the validity of a given device based on certain credentials. Authentication ensures that the access to the designated IoT systems is provided to the authorized users only. Manual authentication becomes a challenge, considering a substantial increase in the number of the IoT devices. Therefore, more efficient authentication mechanisms are required to assure the system security without consuming a significant amount of energy (Khan and Salah, 2018; Aboti, 2020; Imdad et al., 2020).
- **Countermeasures**: There are many different types of attacks that could affect the IoT-based technologies, including malicious scripts, data distortion attacks, DoS attacks, DDoS attacks, eavesdropping attacks, wormhole attacks, sinkhole attacks, jamming attacks, replay attacks, and many others (Farooq et al., 2015; Lee and Lee, 2015; Wahid and Kumar, 2015; Hengst, 2016; Imdad et al., 2020; Abosata et al., 2021). Each attack has its own features and may affect different layers of the IoT architecture. Various countermeasures have been used to address these attacks, such as encryption, IP security, intrusion prevention, intrusion detection, and authentication (Abosata et al., 2021). Considering an increasing amount of the IoT-connected devices, new types of countermeasures should be developed in the following years to protect the IoT architecture layers from malicious attacks.
- **Multiple verticals**: The IoT-based systems have a wide range of applications (or verticals), including railway operations, railway maintenance, demand forecasting, automation, smart cities, energy, and many others. The privacy and security requirements applicable to one vertical may not work well for another vertical (Dabbagh and Rayes, 2019). The future IoT systems should be designed considering vertical-specific privacy and security requirements.
- **User awareness trainings**: Detailed user awareness trainings should be developed and administered to ensure that future users have a clear understanding of the IoT technology to be used and its potential vulnerabilities (Polat and Sodah, 2019). The users should be aware of the security measures implemented by the vendors for a given IoT device as well as realize additional actions that could be taken to improve security and privacy even further.

4.2.4. Standardization and legal challenges

- **Standardization**: Standardization is one of the critical elements that substantially affects the development and deployment of IoT systems. Having a unique standard is essential, so all the relevant actors could easily access and use a given IoT system. Coordination of proposals and standards will facilitate the development of effective IoT infrastructures, services, applications, and devices. The developed standards should be open to all the relevant representatives of a given enterprise. Furthermore, global standards are expected to be more efficient compared to local standards, as global standards will be publicly available to all the relevant IoT users across the globe at no cost (Chen et al., 2014a). Various entities, including the European Telecommunications Standards Institute and the Internet Engineering Task Force, are making efforts towards the development of IoT standards (Rehman et al., 2017). However, making these standards universally applicable still remains a major challenge.
- **Modifying the existing laws and regulations**: Some of the existing laws and regulations for the IoT technologies are rather limited, fairly slow, and too instrumental in many instances (Van Kranenburg and Bassi, 2012). More effective laws and regulations should be designed in the near future in coordination with relevant stakeholders to facilitate the development and deployment of the IoT technologies.
- **Compliance**: Many IoT applications collect and store certain personal information regarding daily activities of people in various geographical locations (e.g., travel history, household energy utilization). Some individuals consider this information as private and do not prefer disclosing it. When such information is moved to the internet via the IoT applications, there is a possibility of privacy violation. Different countries have various requirements regarding privacy policies. Therefore, the future IoT-based technologies should be developed considering the existing privacy policies to ensure that the confidential information will not be disclosed to unauthorized users (Udoh and Kotonya, 2018).
- **Sanctions**: The future development and deployment of the next generation IoT systems will require changes in laws (Rehman et al., 2017). Sanctions should be introduced in case of law violations. There should be a global accountability related to legal issues for using the IoT-based technologies.

4.2.5. Other challenges

- **Business challenges**: Business models and application scenarios are generally clear for mature applications. However, when it comes to the IoT-based applications, there are many uncertainties associated with the selection of the appropriate business model and the application scenario. One IoT solution may not be able to cover multiple application scenarios. Traditional business models may not be effective for the IoT-based applications. Some small-size IoT applications demonstrated their potential for certain industries but did not work well for some other industries. Therefore, all the relevant business aspects should be carefully considered, especially at early stages of the IoT development, in order to decrease the probability of failure and potential monetary losses (Chen et al., 2014a).
- **Global cooperation challenges**: Global cooperation challenges are associated with coordinated efforts by the global community to align broader investments into the IoT infrastructure. There are different approaches that are used for the IoT infrastructure investments (Van Kranenburg and Bassi, 2012). The U.S. primarily relies on an

opportunity investment approach which is based on short- or mid-term return on investment. China adopted an integrated approach to allocate broader investments in the IoT systems (i.e., integrate the IoT with other components). On the other hand, Europe uses a stakeholder approach that supports private–public partnerships and vertical investments by means of four-year plans. The challenging issue is to determine a set of principles that could be used to effectively align these perspectives.

- **Chaos effect**: The growing technological innovations in the field of chips, sensors, and cutting-edge wireless communication technologies have been observed over the last years. However, these new technologies have come with some of the biggest challenges, such as competing protocols and standards, issues related to privacy and security, complex communications, and testing issues for the IoT devices. A minor error can cause a significant disruption in the whole system within the hyper-connected IoT world and result in catastrophic consequences for transportation, health, industry, and many other domains (Lee and Lee, 2015). In order to avoid the "chaos effect", relevant stakeholders should improve standardization and security of applications, decrease the complexity of connected systems, and guarantee privacy and safety of the user information.
- **Ethical issues**: Along with privacy issues, there are many other ethical challenges that are associated with the IoT-based technologies, including the following (Habibipour et al., 2019): secret recording or videotaping, collection of unnecessary data, secondary use of data, personal data leakage, and intellectual property rights issues. The existing ethical issues should be effectively addressed by relevant stakeholders to facilitate the development and deployment of the IoT-based technologies.
- **Ecological issues**: The deployment of IoT technologies may cause a variety of ecological issues that include, but are not limited to, the following (Tzafestas, 2018; Habibipour et al., 2019): high power consumption, battery life and heating, software reusability, reusability of materials, and waste. Innovative approaches should be developed to ensure sustainable deployment of the IoT-based technologies and preserve the environment.
- **Interactions with humans**: Many IoT applications do not operate by themselves and require some inputs from humans (e.g., many healthcare services are based on human-device interactions, where the IoT application assists a human operator to perform certain tasks). Interactions between IoT applications and humans are complex and have to be harmonized. An accurate modeling of human behavior still remains a quite difficult task (Udoh and Kotonya, 2018). New approaches are needed to simulate human behavior and improve human-device interactions.
- **User perception and confidence**: There is no technology that cannot be compromised in any way. The IoT technologies are viewed as complex systems, and there are always concerns regarding safety and security of the information. Moreover, users may have doubts regarding the technology performance under disrupted and emergency conditions (Fraszczyk et al., 2015; Fraszczyk and Mulley, 2017; Singh et al., 2021a). New educational programs should be developed to improve user perception and confidence in the IoT technologies. The future users should be also involved even in testing phases to ensure that they will be comfortable with the next generation IoT technologies and autonomous systems in rail transportation and other domains (Henne et al., 2019; Singh et al., 2021a).

5. Concluding remarks and future research needs

The Internet of Things (IoT) applications have become an integral part of human life. The internet is a very powerful tool that continuously allows improving living standards of many countries across the globe. Anything can communicate with the internet at any time at any place in order to provide certain services or information to anyone by any network. Such a phenomenon serves as a foundation for the IoT. The growth of IoT-based technologies is anticipated to be much faster than before due to the development of new generation technologies (e.g., the sixth generation technology, the seventh generation technology, and federated learning). These technologies have the potential for the IoT applications to run in a safer, faster, and more reliable way beyond imagination. The IoT has been heavily used in different domains, including education, business, transportation, infrastructure, smart cities, commercial, healthcare, and government. The IoT applications have been used in the railway industry as well, including railway operations, maintenance, management, train control, and video surveillance. Although several studies have been conducted to date and discussed the use of different IoT technologies, no significant efforts have been made towards developing a detailed understanding of the IoT applications specifically in the railway industry and how these applications could facilitate sustainable railway operations.

Considering such a shortcoming, this study conducted a comprehensive and holistic review of the state-of-the-practice and the state-of-the-art to identify the existing IoT technologies, applications of various IoT technologies, current trends in the deployment of IoT technologies for railway-specific needs along with the associated next generation technologies, main challenges, and opportunities for the future research. The present survey identified many advantages of the IoT applications for railway transportation systems (e.g., effective management of railway operations, enhanced monitoring and maintenance, improved safety and level of service, and sustainable development). However, a variety of challenges were discovered as well, including technological challenges, operational challenges, privacy and security challenges, standardization and legal challenges, and other challenges. These challenges must be addressed by relevant stakeholders in the near future to assure sustainable development and deployment of the IoT applications in railway transportation systems and other domains.

The findings from the conducted survey are anticipated to provide important insights regarding the applicability of IoT technologies in the railway industry and other related domains, their future potential, operational benefits to relevant authorities and stakeholders, as well as critical future research needs that require attention. This study can be expanded further in different directions, including but not limited to the following:

- o Assess new types of hardware that can be potentially used for the new generation IoT technologies. Since one of the objectives in the development of future IoT technologies is to reduce the size of devices and their cost, advanced types of hardware technologies should be considered (e.g., nanotechnology-based hardware technologies). Furthermore, new mechanisms for ultra-low power consumption should be investigated as well.
- o New types of artificial intelligence-based algorithms can be developed and evaluated for self-adaptive, self-optimizing, self-configuring, and self-protecting IoT networks as a part of future research. Such algorithms would be essential considering highly dynamic nature of the IoT environment.
- o The future research should focus on the development of new types of security and privacy policies that will be user-centric. In particular, each user of a given IoT device should have a flexibility of selecting a specific user profile based on the user security and privacy preferences (e.g., more restrictive security and privacy measures will be applied if a user decides to have a high priority for security and privacy).
- o More effective methodologies can be explored for digital and real-time mapping, device discovery, semantic search operations, and universal authentication. Such methodologies would facilitate sustainable development and deployment of the IoT applications in railway transportation systems and other domains.
- o Evaluate new types of alternatives that can effectively address the issues associated with energy consumption for the IoT-based

technologies (e.g., energy-harvesting methods, collaborative resource sharing when multiple IoT devices can effectively share the available energy between each other in order to complete particular tasks and services).

- Different types of drones have been widely used for monitoring various operations in different domains and inspection of specific assets (Macrina et al., 2020; Pasha et al., 2022b). The future research should explore the potential of integrating drones with the IoT technologies for improved monitoring of railway operations.
- Many studies have been conducted to date aiming to improve social, environmental, and economic sustainability of various supply chain operations (Govindan et al., 2013; Edalatpour et al., 2018; Fathollahi-Fard et al., 2021b). A simultaneous consideration of the aforementioned sustainability dimensions is also referred to as a "triple bottom line approach". The future research should concentrate more on how the IoT technologies could facilitate the development and deployment of triple bottom line approaches for sustainable railway transportation.
- Rail transportation has been substantially impacted by the COVID-19 pandemic (Othman, 2021). The ridership in public rail transit systems substantially declined, especially during the COVID-19 lockdown periods. There is always a concern of potential spread of airborne diseases in public rail transit systems and other transit systems as well. The future studies could explore the potential of using various IoT technologies and contact tracing methods for preventing the spread of viruses and improve the resilience of railway transportation systems to the future pandemics.
- Perform a set of interviews with various stakeholders (e.g., researchers, railway companies, government representatives) to determine the key legal challenges that affect the development and deployment of the IoT technologies across the globe and present a set of recommendations based on the information obtained.
- Perform a set of interviews with the existing and potential IoT users to investigate their perception towards the current IoT technologies and new generation IoT technologies that will be on the market in the following years. A diverse group of individuals should be considered (i.e., individuals of different age, gender, education, nationality, etc.). Such interviews can assist with the identification of factors that directly influence user perception towards the IoT technologies and can be further used by the appropriate stakeholders.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This study was partially supported by the Florida Department of Transportation (grants BDV30-977-26 and BDV30-977-33). The opinions, findings and conclusions expressed in this publication are those of the authors and not necessarily those of the Florida Department of Transportation or the U.S. Department of Transportation.

Appendix

Abbreviations Used

3D	- Three-Dimensional
3G	- the Third Generation Technology
4G	- the Fourth Generation Technology
5G	- the Fifth Generation Technology
6G	- the Sixth Generation Technology
7G	- the Seventh Generation Technology
AI	- Artificial Intelligence
AMELIA	- Aircraft Monitoring and Electronically Linked Instantaneous Analytics
AR	- Augmented Reality
B2C	- Business-to-Consumer
BI	- Business Intelligence
CA	- Certificate Authority
CERP-IoT	- Cluster of European Research Projects on the Internet of Things
CR	- Cognitive Radio
D2D	- Device-to-Device
DDoS	- Distributed Denial-of-Service
DGPS	- Differential Global Positioning System
DoS	- Denial-of-Service
DOT	- Department of Transportation
DSRC	- Dedicated Short-Range Communications
ED	- External Devices
FDAU	- Flight Data Acquisition Unit
FL	- Federated Learning
FOS	- Fiber Optic Sensing
GE	- Gigabit Ethernet
GHz	- Gigahertz
G-IoT	- Green Internet of Things
GPRS	- General Packet Radio Services
GPS	- Global Positioning System
GSM	- Global System for Mobile Communication
HBF	- Holographic Beamforming
HF	- High Frequency
H-IoT	- Healthcare IoT
IIoT	- Industrial Internet of Things
IoRT	- Internet of Railway Things
IoT	- Internet of Things

(*continued on next page*)

(*continued*)

IoVT	- Internet of Video Things
IP	- Internet Protocol
IT	- Information Technology
ITS	- Intelligent Transportation Systems
LAN	- Local Area Networks
LPWAN	- Low-Power Wide-Area Networks
LTE	- Long-Term Evolution
MIMO	- Multiple-Input-Multiple-Output
MITM	- Man-in-the-Middle
ML	- Machine Learning
MQTT	- Message Queuing Telemetry Transport
NFC	- Near Field Communications
NFV	- Network Function Virtualization
PQM	- Product Quality Management
QoS	- Quality of Service
RFID	- Radio Frequency Identification System
RIoT	- Rail Internet of Things
SDN	- Software Defined Networking
SFI	- Software Fault Injection
SG	- Smart Grid
SNCF	- The Société Nationale des Chemins de Der Français
SOA	- Service-Oriented Architecture
THz	- Terahertz
UAV	- Unmanned Aerial Vehicle
U.S.	- United States
V2V	- Vehicle-to-Vehicle
V2X	- Vehicle-to-Everything
WiFi	- Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WiRF	- Wireless Radio Frequency
WLAN	- Wireless Local-Area Network
WSN	- Wireless Sensor Networks
WSS	- Wireless Smart Sensors

References

Abioye, O.F., Dulebenets, M.A., Pasha, J., Kavoosi, M., Moses, R., Sobanjo, J., Ozguven, E.E., 2020. Accident and hazard prediction models for highway–rail grade crossings: a state-of-the-practice review for the USA. Railway Eng. Sci. 28 (3), 251–274.

Abosata, N., Al-Rubaye, S., Inalhan, G., Emmanouilidis, C., 2021. Internet of things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors 21 (11), 3654.

Aboti, C.D., 2020. Studies of challenges to mitigating cyber risks in iot-based commercial aviation. Int. J. Sci. Res. Develop. 7, 133–139.

Adebiyi, O.O., Cruz, M., 2018. Green sustainability development for industry internet of things in railway transportation industry. Int. J. Trend Sci. Res. Develop. 3 (1), 203–208.

Adeel, A., Gogate, M., Farooq, S., Ieracitano, C., Dashtipour, K., Larijani, H., Hussain, A., 2019. A survey on the role of wireless sensor networks and IoT in disaster management. In *Geological disaster monitoring based on sensor networks* (pp. 57-66). Springer, Singapore.

Adil, M., Khan, M.K., 2021. Emerging IoT applications in sustainable smart cities for COVID-19: network security and data preservation challenges with future directions. Sustain. Cities Soc., 103311

Ahmed, E., Yaqoob, I., Hashem, I.A.T., Khan, I., Ahmed, A.I.A., Imran, M., Vasilakos, A. V., 2017. The role of big data analytics in Internet of Things. Comput. Netw. 129, 459–471.

Ai, B., Guan, K., Rupp, M., Kurner, T., Cheng, X., Yin, X.F., Wang, Q., Ma, G.Y., Li, Y., Xiong, L., Ding, J.W., 2015. Future railway services-oriented mobile communications network. IEEE Commun. Mag. 53 (10), 78–85.

Ai, B., Molisch, A.F., Rupp, M., Zhong, Z.D., 2020. 5G key technologies for smart railways. Proc. IEEE 108 (6), 856–893.

Akyildiz, I.F., Kak, A., Nie, S., 2020. 6G and beyond: the future of wireless communications systems. IEEE Access 8, 133995–134030.

AL Enterprise.com, The Internet of Things in Transportation. [online]. Available at 2020.

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., Al-Jaroodi, J., 2015. Applications of big data to smart cities. J. Internet Serv. Appl. 6 (1), 1–15.

Alagarsamy, S., Kandasamy, R., Subbiah, L. and Palanisamy, S., 2019. Applications of Internet of Things in Pharmaceutical Industry. *Available at SSRN 3441099*.

Alam, S., Chowdhury, M.M., Noll, J., 2011. Interoperability of security-enabled internet of things. Wireless Pers. Commun. 61 (3), 567–586.

Alcaraz, C., Najera, P., Lopez, J., Roman, R., 2010. Wireless sensor networks and the internet of things: Do we need a complete integration? 1st International Workshop on the Security of the Internet of Things (SecIoT'10).

Ali, Z.H., Ali, H.A., Badawy, M.M., 2015. Internet of Things (IoT): definitions, challenges and recent research directions. Int. J. Comp. Appl. 128 (1), 37–47.

Alrawais, A., Alhothaily, A., Hu, C., Cheng, X., 2017. Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput. 21 (2), 34–42.

Aono, K., Lajnef, N., Faridazar, F. and Chakrabartty, S., 2016, May. Infrastructural health monitoring using self-powered internet-of-things. In *2016 IEEE international symposium on circuits and systems (ISCAS)* (pp. 2058-2061). IEEE.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58.

Armentia, A., Gangoiti, U., Priego, R., Estévez, E., Marcos, M., 2015. Flexibility support for homecare applications based on models and multi-agent technology. Sensors 15 (12), 31939–31964.

Arunjyothi, B., Harikrishna, B., 2020. Automated railway gate control using internet of things. In: Soft Computing: Theories and Applications. Springer, Singapore, pp. 501–513.

Aslam, S., Michaelides, M.P., Herodotou, H., 2020. Internet of ships: a survey on architectures, emerging applications, and challenges. IEEE Internet Things J. 7 (10), 9714–9727.

Atlam, H.F. and Wills, G.B., 2019. Technical aspects of blockchain and IoT. In *Advances in Computers* (Vol. 115, pp. 1-39). Elsevier.

Atlam, H.F., Walters, R.J., Wills, G.B., 2018. Fog computing and the internet of things: areview. Big Data Cognitive Comput. 2 (2), 10.

Awoyemi, B.S., Alfa, A.S., Maharaj, B.T., 2020. Resource optimization in 5G and internet-of-things networking. Wireless Pers. Commun. 111 (4), 2671–2702.

Aziz, A.A., Mohamad, K.A., Alias, A., 2020. Obstacle detection system for railways using IoT sensors. Evol. Elec. Electron. Eng. 1 (1), 57–63.

Badarinath, R., Prabhu, V.V., 2017, September. Advances in Internet of Things (IoT) in manufacturing. In *IFIP International Conference on Advances in Production Management Systems* (pp. 111-118). Springer, Cham.

Bali, A., Raina, M., Gupta, S., 2018. Study of various applications of Internet of Things (IoT). Int. J. Comput. Eng. Technol. 9 (2), 39–50.

Bansal, N., Lal, T., 2019. A Brief Review on the Future and Challenges of Internet of Things (IoT). Pannonian Conference on Advances in Information Technology (PCIT 2019), Veszprém, Hungary.

Bellavista, P., Cardone, G., Corradi, A., Foschini, L., 2013. Convergence of MANET and WSN in IoT urban scenarios. IEEE Sens. J. 13 (10), 3558–3567.

Besher, K.M., Nieto-Hipolito, J.I., Buenrostro-Mariscal, R., Ali, M.Z., 2021. Spectrum Based Power Management for Congested IoT Networks. Sensors 21 (8), 2681.

Bessis, N., Dobre, C. (Eds.), 2014. Big Data and Internet of Things: A Roadmap for Smart Environments (Vol. 546). Springer International Publishing, Basel, Switzerland.

Bogaard, P., 2020. IoT Proving Its Worth to Rail Industry at a Time of Crisis. [online]. Available: https://www.railtech.com/ digitalisation/2020/04/14.

Cabra, J., Castro, D., Colorado, J., Mendez, D. and Trujillo, L., 2017, June. An IoT approach for wireless sensor networks applied to e-health environmental monitoring. In *2017 IEEE International Conference on Internet of Things (iThings) and*

IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 578-583). IEEE.
Castillo, F.R.P., 2019. The sixth sensor: How IoT smart sensors can address operational challenges introduced by increasing automation in railways. [online]. Available at: https://railsystemsaustralia.com.au/.
Chapman, L., Bell, S.J., 2018. High-resolution monitoring of weather impacts on infrastructure networks using the Internet of Things. Bull. Am. Meteorol. Soc. 99 (6), 1147–1154.
Chapman, L., Warren, E. and Chapman, V., 2016. Using the internet of things to monitor low adhesion on railways. In *Proceedings of the Institution of Civil Engineers-Transport* (Vol. 169, No. 5, pp. 321-329). Thomas Telford Ltd.
Chen, C.W., 2020. Internet of video things: Next-generation IoT with visual sensors. IEEE Internet Things J. 7 (8), 6676–6685.
Chen, S., Xu, H., Liu, D., Hu, B., Wang, H., 2014a. A vision of IoT: Applications, challenges, and opportunities with china perspective. IEEE Internet Things J. 1 (4), 349–359.
Chen, Y., Han, F., Yang, Y.H., Ma, H., Han, Y., Jiang, C., Lai, H.Q., Claffey, D., Safar, Z., Liu, K.R., 2014b. Time-reversal wireless paradigm for green internet of things: An overview. IEEE Internet Things J. 1 (1), 81–98.
Choi, N., Kim, D., Lee, S.J., Yi, Y., 2017. A fog operating system for user-oriented iot services: Challenges and research directions. IEEE Commun. Mag. 55 (8), 44–51.
Chu, Y., Pan, L., Leng, K., Fu, H.C., Lam, A., 2020. Research on key technologies of service quality optimization for industrial IoT 5G network for intelligent manufacturing. Int. J. Adv. Manuf. Technol. 107 (3), 1071–1080.
Dabbagh, M., Rayes, A., 2019. Internet of things security and privacy. In *Internet of Things from hype to reality* (pp. 211-238). Springer, Cham.
Darshan, K.R. and Anandakumar, K.R., 2015. A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)* (pp. 132-136). IEEE.
Deebak, B.D., Al-Turjman, F., 2020. Drone of IoT in 6G wireless communications: Technology, challenges, and future aspects. In: Unmanned Aerial Vehicles in Smart Cities. Springer, Cham, pp. 153–165.
Deng, N., 2012, August. RFID technology and network construction in the internet of things. In *2012 International Conference on Computer Science and Service System* (pp. 979-982). IEEE.
D'Errico, L., Franchi, F., Graziosi, F., Rinaldi, C. and Tarquini, F., 2017, July. Design and implementation of a children safety system based on IoT technologies. In *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)* (pp. 1-6). IEEE.
Dhande, B.S., Pacharaney, U.S., 2017. Railway management system using IR sensors and internet of things technology. Int. J. Sci. Res. Network Secur. Commun. 5 (1), 12–15.
Dillon, T., Wu, C. and Chang, E., 2010, April. Cloud computing: issues and challenges. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 27-33). IEEE.
Dirnfeld, R., Flammini, F., Marrone, S., Nardone, R. and Vittorini, V., 2020. Low-power wide-area networks in intelligent transportation: Review and opportunities for smart-railways. In *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)* (pp. 1-7). IEEE.
Dulebenets, M.A., 2018. A comprehensive multi-objective optimization model for the vessel scheduling problem in liner shipping. Int. J. Prod. Econ. 196, 293–318.
Dulebenets, M.A., 2019. A Delayed Start Parallel Evolutionary Algorithm for just-in-time truck scheduling at a cross-docking facility. Int. J. Prod. Econ. 212, 236–258.
Dulebenets, M.A., 2021. An Adaptive Polyploid Memetic Algorithm for scheduling trucks at a cross-docking terminal. Inf. Sci. 565, 390–421.
Economides, A.A., 2016, July. User perceptions of Internet of Things (IoT) systems. In *International Conference on E-Business and Telecommunications* (pp. 3-20). Springer, Cham.
Edalatpour, M.A., Mirzapour Al-e-Hashem, S.M.J., Karimi, B., Bahli, B., 2018. Investigation on a novel sustainable model for waste management in megacities: A case study in Tehran municipality. Sustainable Cities Soc. 36, 286–301.
Eiza, M.H., Randles, M., Johnson, P., Shone, N., Pang, J. and Bhih, A., 2015. Rail internet of things: An architectural platform and assured requirements model. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* (pp. 364-370). IEEE.
Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A., 2018. Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6, 20596–20608.
Elmeadawy, S. and Shubair, R.M., 2019, November. 6G wireless communications: Future technologies and research challenges. In *2019 international conference on electrical and computing technologies and applications (ICECTA)* (pp. 1-5). IEEE.
Elmustafa, S.A.A., Mujtaba, E.Y., 2019. Internet of things in smart environment: Concept, applications, challenges, and future directions. World Scientific News 134 (1), 1–51.
Ephrem, E., 2015. Architecture of Wireless Sensor Networks. [online]. Available at: http://servforu.blogspot.com.tr/2012/12/architecture-of-wirelesssensor-networks.html.
Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T., 2015. A review on internet of things (IoT). Int. J. Comp. Appl. 113 (1), 1–7.
Fathollahi-Fard, A.M., Dulebenets, M.A., Hajiaghaei-Keshteli, M., Tavakkoli-Moghaddam, R., Safaeian, M., Mirzahosseinian, H., 2021a. Two hybrid meta-heuristic algorithms for a dual-channel closed-loop supply chain network design problem in the tire industry under uncertainty. Adv. Eng. Inf. 50, 101418.
Fathollahi-Fard, A.M., Woodward, L., Akhrif, O., 2021b. Sustainable distributed permutation flow-shop scheduling model based on a triple bottom line concept. J. Ind. Inf. Integr. 24, 100233.
Flammini, F., Lin, Z., Vittorini, V., 2020. Roadmaps for AI integration in the rail sector—Rails. ERCIM News 2020 (121).
Fraga-Lamas, P., Fernández-Caramés, T.M., Castedo, L., 2017. Towards the Internet of smart trains: a review on industrial IoT-connected railways. Sensors 17 (6), 1457.
Fraszczyk, A., Mulley, C., 2017. Public perception of and attitude to driverless train: a case study of Sydney, Australia. Urban Rail Transit 3 (2), 100–111.
Fraszczyk, A., Brown, P., Duan, S., 2015. Public perception of driverless trains. Urban Rail Transit 1 (2), 78–86.
Ganga, A., Periasamy, J.K., Gopinath, N., Sathishkumar, D., 2019. IoT based passenger comfort and services in railways. Int. J. Recent Technol. Eng. 8 (4), 7081–7084.
Gangwar, N., Semwal, T., Nair, S.B., 2017. CARE: An IoT based system for passenger service and comfort in railways. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 55-62). IEEE.
Gharami, S., Prabadevi, B., Bhimnath, A., 2019. Semantic analysis-internet of things, study of past, present, and future of IoT. Electronic Government, Int. J. 15 (2), 144–165.
Gholizadeh, H., Fazlollahtabar, H., Fathollahi-Fard, A.M., Dulebenets, M.A., 2021. Preventive maintenance for the flexible flowshop scheduling under uncertainty: a waste-to-energy system. Environ. Sci. Pollut. Res. 1–20.
Gia, T.N., Jiang, M., Sarker, V.K., Rahmani, A.M., Westerlund, T., Liljeberg, P. and Tenhunen, H., 2017, June. Low-cost fog-assisted healthcare IoT system with energy-efficient sensor nodes. In *2017 13th international wireless communications and mobile computing conference (IWCMC)* (pp. 1765-1770). IEEE.
Govindan, K., Khodaverdi, R., Jafarian, A., 2013. A fuzzy multi criteria approach for measuring sustainability performance of a supplier based on triple bottom line approach. J. Cleaner Prod. 47, 345–354.
Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29 (7), 1645–1660.
Habibipour, A., Padyab, A.M. and Ståhlbröst, A., 2019. Social, ethical and ecological issues in wearable technologies. In *AMCIS 2019, Twenty-fifth Americas Conference on Information Systems, Cancun, México, Augusti 15-17, 2019*. Association for Information Systems.
Hashem, I.A.T., Chang, V., Anuar, N.B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., Chiroma, H., 2016. The role of big data in smart city. Int. J. Inf. Manage. 36 (5), 748–758.
Hengst, K., 2016. DDoS through the Internet of Things, An analysis determining the potential power of a DDoS attack using IoT devices. Twente Student Conference on IT.
Henne, M., Schwaiger, A., Weiss, G., 2019. Managing Uncertainty of AI-based Perception for Autonomous Systems. In *AISafety, IJCAI*, vol. 2419, August 2019.
Hsu, C.J., Jones, E.G., 2017. Transmission range evaluations for connected vehicles at highway-rail grade crossings. Designs 1 (1), 2.
Husamuddin, M., Qayyum, M., 2017. Internet of Things: A study on security and privacy threats. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 93-97). IEEE.
IBM, 2021. Blockchain overview. [online]. Available at: https://www.ibm.com/topics/what-is-blockchain.
Imdad, M., Jacob, D.W., Mahdin, H., Baharum, Z., Shaharudin, S.M., Azmi, M.S., 2020. Internet of things (IoT); security requirements, attacks, and counter measures. Indonesian J. Elec. Eng. Computer Sci. 18 (3), 1520–1530.
Islam, M.M., Rahaman, A., Islam, M.R., 2020. Development of smart healthcare monitoring system in IoT environment. SN Comp. Sci. 1, 1–11.
Ivezic, N., Kulvatunyou, B., Srinivasan, V., 2014. On architecting and composing through-life engineering information services to enable smart manufacturing. Procedia Cirp 22, 45–52.
Jadeja, Y. and Modi, K., 2012, March. Cloud computing-concepts, architecture, and challenges. In *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)* (pp. 877-880). IEEE.
Jamkhaneh, H.B., Shahin, R., Tortorella, G.L., 2022. Analysis of Logistics 4.0 Service Quality and its sustainability enabler scenarios in emerging economy. Cleaner Logistics Supply Chain 4, 100053.
Jauro, F., Chiroma, H., Gital, A.Y., Almutairi, M., Shafi'i, M.A. and Abawajy, J.H., 2020. Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend. *Applied Soft Computing*, *96*, p.106582.
Ji, X., Huang, K., Jin, L., Tang, H., Liu, C., Zhong, Z., You, W., Xu, X., Zhao, H., Wu, J., Yi, M., 2018. Overview of 5G security technology. Sci. China Inf. Sci. 61 (8), 1–25.
Jia, X., Feng, Q., Fan, T. and Lei, Q., 2012, April. RFID technology and its applications in Internet of Things (IoT). In *2012 2nd international conference on consumer* electronics, *communications, and networks (CECNet)* (pp. 1282-1285). IEEE.
Jimenez, F. and Torres, R., 2015, November. Building an IoT-aware healthcare monitoring system. In *2015 34th International Conference of the Chilean Computer Science Society (SCCC)* (pp. 1-4). IEEE.
Jo, O., Kim, Y.K., Kim, J., 2017. Internet of things for smart railway: feasibility and applications. IEEE Internet Things J. 5 (2), 482–490.
Karaduman, G., Karakose, M. and Akin, E., 2018. Condition monitoring platform in railways based on IoT. In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)* (pp. 1-4). IEEE.
Karthikeyyan, P., Velliangiri, S., 2019, July. Review of Blockchain based IoT application and its security issues. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 6-11). IEEE.
Kaur, S., Singh, I., 2016. A survey report on Internet of Things applications. Int. J. Comput. Sci. Trends Technol. 4 (2), 330–335.
Kavoosi, M., Dulebenets, M.A., Abioye, O., Pasha, J., Theophilus, O., Wang, H., Kampmann, R., Mikijeljević, M., 2020a. Berth scheduling at marine container

terminals: A universal island-based metaheuristic approach. Maritime Business Rev. 5 (1), 30–66.
Kavoosi, M., Dulebenets, M.A., Abioye, O.F., Pasha, J., Wang, H., Chi, H., 2019. An augmented self-adaptive parameter control in evolutionary computation: A case study for the berth scheduling problem. Adv. Eng. Inf. 42, 100972.
Kavoosi, M., Dulebenets, M.A., Pasha, J., Abioye, O.F., Moses, R., Sobanjo, J., Ozguven, E.E., 2020b. Development of algorithms for effective resource allocation among highway–rail grade crossings: a case study for the State of Florida. Energies 13 (6), 1419.
Khan, M.A., Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Syst. 82, 395–411.
Khutey, R., Rana, G., Dewangan, V., Tiwari, A., Dewamngan, A., 2015. Future of wireless technology 6G & 7G. Int. J. Elec. Electron. Res. 3 (2), 583–585.
Kimiagar, Y., 2019. What are the Artificial Intelligence Applications in Rail Transit? [online]. Available: https://www.apta.com/wpcontent/uploads/What-are-the-Artificial-Intelligence-Applicationsin-Rail-Transit_Yousef_Kimiagar.pdf.
Kocakulak, M., Butun, I., 2017, January. An overview of Wireless Sensor Networks towards internet of things. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)* (pp. 1-6). IEEE.
Kortuem, G., Kawsar, F., Sundramoorthy, V., Fitton, D., 2009. Smart objects as building blocks for the internet of things. IEEE Internet Comput. 14 (1), 44–51.
Kumar, M., Annoo, K., Mandal, R.K., 2018. The Internet of Things applications for challenges and related future technologies & development. Int. Res. J. Eng. Technol. 5 (1).
Kumar, M., Arora, S., Verma, A., 2020. IoT remote tracking and increased adaptive fluctuating operation of the maglev train network medium-low speed train. Int. J. Adv. Res. Eng. Technol. 11 (12), 1724–1729.
Kumar, N.M., Mallick, P.K., 2018. Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. 132, 1815–1823.
Lambert, S., 2020. Using the Internet of Things to Transform Railways. [online]. Available: https://www.mes-insights.com/using-the-internetof-things-to-transform-railways-a-956212.
Lampropoulos, G., Siakas, K., Anastasiadis, T., 2018. Internet of Things (IoT) in industry: Contemporary application domains, innovative technologies, and intelligent manufacturing. Int. J. Adv. Sci. Res. Eng. 4 (10), 109–118.
Lanzisera, S., Weber, A.R., Liao, A., Pajak, D., Meier, A.K., 2014. Communicating power supplies: Bringing the internet to the ubiquitous energy gateways of electronic devices. IEEE Internet Things J. 1 (2), 153–160.
Lee, I., Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horiz. 58 (4), 431–440.
Lei, X., Wang, X.F. and Li, L., 2013. Railway information integration and sharing mode researching based on internet of things. In *Advanced Materials Research* (Vol. 694, pp. 3353-3356). Trans Tech Publications Ltd.
Leles, R.D.C., Rodrigues, J.J., Woungang, I.W., Rabel, R.A. and Furtado, V., 2018. Railways networks-challenges for IoT underground wireless communications. In *2018 IEEE 10th Latin-American Conference on Communications (LATINCOM)* (pp. 1-6). IEEE.
Li, Q.Y., Zhong, Z.D., Liu, M. and Fang, W.W., 2017. Smart railway based on the Internet of Things. In *Big data analytics for sensor-network collected intelligence* (pp. 280-297). Academic Press.
Li, S., Da Xu, L. and Zhao, S., 2015. The internet of things: a survey. *Inf. Syst. Front.*, *17* (2), pp.243-259.
Li, S., Da Xu, L. and Zhao, S., 2018. 5G Internet of Things: A survey. *J. Ind. Inform. Integr.*, *10*, pp.1-9.
Li, W., Kara, S., 2017. Methodology for monitoring manufacturing environment by using wireless sensor networks (WSN) and the internet of things (IoT). Procedia CIRP 61, 323–328.
Li, W., Chen, Z.H. and Sui, L.Y., 2014. Design and Application of Mass Passenger Flow Precautionary and Forecasting System in Rail Transit Based on the Internet of Things Technology. In *Applied Mechanics and Materials* (Vol. 556, pp. 6366-6369). Trans Tech Publications Ltd.
Ling, Z.H.A.O., 2013. Design of railway freight transport security system based on internet of things. J. Chongqing Univ. Technol. (Natural Science) 6, 025.
Liu, X., Zhang, X., Xue, F., Liao, W., 2010. United Transportation of Railways and Highways Omni distance Tracking System Model under the Internet of Things. In: ICLEM 2010: Logistics For Sustained Economic Development: Infrastructure, pp. 2207–2213.
Liu, Y., Yuan, X., Xiong, Z., Kang, J., Wang, X., Niyato, D., 2020. Federated learning for 6G communications: Challenges, methods, and future directions. China Commun. 17 (9), 105–118.
Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L., 2015. Fog computing: Focusing on mobile users at the edge. *arXiv preprint arXiv:1502.01815*.
Mahmoud, H.H.H., Amer, A.A., Ismail, T., 2021. 6G: A comprehensive survey on technologies, applications, challenges, and research problems. Trans. Emerg. Telecommun. Technol. 32 (4), e4233.
Mainetti, L., Patrono, L. and Vilei, A., 2011, September. Evolution of wireless sensor networks towards the internet of things: A survey. In *SoftCOM 2011, 19th international conference on software, telecommunications and computer networks* (pp. 1-6). IEEE.
Malik, U.M., Javed, M.A., Zeadally, S. and ul Islam, S., 2021. Energy efficient fog computing for 6G enabled massive IoT: Recent trends and future opportunities. *IEEE Internet of Things Journal*, pp.1-22.
Macrina, G., Pugliese, L., Guerriero, F., Laporte, G., 2020. Drone-aided routing: a literature review. Transp. Res. Part C: Emerg. Technol. 120, 102762.
Mc Gee, K., Anandarajah, P., Collins, D., 2019. A review of chipless remote sensing solutions based on RFID technology. Sensors 19 (22), 4829.
Mehmood, M.Y., Oad, A., Abrar, M., Munir, H.M., Hasan, S.F., Muqeet, H. and Golilarz, N.A., 2021. Edge computing for IoT-enabled smart grid. *Security and Communication Networks*, *2021*.
Minoli, D. and Occhiogrosso, B., 2017. Internet of Things (IoT)-Based Apparatus and Method for Rail Crossing Alerting of Static or Dynamic Rail Track Intrusions. In *ASME/IEEE Joint Rail Conference* (Vol. 50718, p. V001T06A016). American Society of Mechanical Engineers.
Mohamed, A., Peng, Q., Abid, M.M., 2020. Integrated maintenance logistics monitoring system for high-speed rail, based on internet of things technology. Eur. TransportTrasporti Europei 2020 (75–6), 1–10.
Monrat, A.A., Schelén, O., Andersson, K., 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 7, 117134–117151.
Mordor Intelligence, 2021. Smart Railways Market - Growth, Trends, Covid-19 Impact, And Forecasts (2021 - 2026). [online]. Available at: https://www.mordorintelligence.com/industry-reports/smart-railways-market.
Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N., Kumar, V., 2017. Security and privacy in fog computing: Challenges. IEEE Access 5, 19293–19304.
Muthuramalingam, S., Bharathi, A., Gayathri, N., Sathiyaraj, R. and Balamurugan, B., 2019. IoT based intelligent transportation system (IoT-ITS) for global perspective: A case study. In *Internet of Things and Big Data Analytics for Smart Generation* (pp. 279-300). Springer, Cham.
Mutlag, A.A., Abd Ghani, M.K., Arunkumar, N.A., Mohammed, M.A., Mohd, O., 2019. Enabling technologies for fog computing in healthcare IoT systems. Future Generation Computer Systems 90, 62–78.
Naser, F., 2018. The Potential Use of Blockchain Technology in Railway Applications: An Introduction of a Mobility and Speech Recognition Prototype. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 4516-4524). IEEE.
Neumeister, D., Campbell, R., Sharkey, J. and Utterback, J., 2019. Prototype Rail Crossing Violation Warning (RCVW) – Advancing the Use of Connected Vehicle Technologies to Prevent Crashes at Rail Grade Crossings by Warning Vehicle Drivers of Predicted Violations. *AREMA 2019 Annual Conference. Minneapolis, MN, USA*.
Ni, J., Zhang, K., Lin, X., Shen, X., 2017. Securing fog computing for internet of things applications: Challenges and solutions. IEEE Commun. Surv. Tutorials 20 (1), 601–628.
Nofer, M., Gomber, P., Hinz, O., Schiereck, D., 2017. Blockchain. *Business & Information*. Systems Eng. 59 (3), 183–187.
Othman, K., 2021. Public acceptance and perception of autonomous vehicles: a comprehensive review. AI Ethics 1 (3), 355–387.
S. Pal A. Dorri R. Jurdak Blockchain for IoT Access Control: Recent Trends and Future Research Directions 2021 arXiv preprint arXiv:2106.04808.
Paragon, The History of Radio Frequency Identification Technology [online]. Available at 2021 https://www.paragon-id.com/en/inspiration/history-radio-frequency-identification-technology.
Park, S.S., 2018, January. An IoT application service using mobile RFID technology. In *2018 International Conference on Electronics, Information, and Communication (ICEIC)* (pp. 1-4). IEEE.
Parvizimosaed, M., Noei, M., Yalpanian, M. and Bahrami, J., 2021, May. A Containerized Integrated Fast IoT Platform for Low Energy Power Management. In *2021 7th International Conference on Web Research (ICWR)* (pp. 318-322). IEEE.
Pasha, J., Dulebenets, M.A., Singh, P., Moses, R., Sobanjo, J., Ozguven, E.E., 2021. Towards improving sustainability of rail transport by reducing traffic delays at level crossings: A case study for the State of Florida. Cleaner Logistics Supply Chain 1, 100001.
Pasha, J., Nwodu, A.L., Fathollahi-Fard, A.M., Tian, G., Li, Z., Wang, H., Dulebenets, M. A., 2022a. Exact and metaheuristic algorithms for the vehicle routing problem with a factory-in-a-box in multi-objective settings. Adv. Eng. Inf. 52, 101623.
Pasha, J., Elmi, Z., Purkayastha, S., Fathollahi-Fard, A.M., Ge, Y.E., Lau, Y.Y., Dulebenets, M.A., 2022b. The drone scheduling problem: a systematic state-of-the-art review. IEEE Trans. Intell. Transp. Syst. 1–24.
Pate, J. and Adegbija, T., 2018, January. AMELIA: An application of the Internet of Things for aviation safety. In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-6). IEEE.
Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., Hassan, M., 2019. The internet of things (IoT) and its application domains. Int. J. Comp. Appl. 975 (8887), 182.
Pirl, L., 2019. Examining Dependability in the Internet of Things. Technical Report: Fall Retreat 2018 (129), 163.
Polat, G., and Sodah, F., 2019. Security issues in IoT: Challenges and countermeasures. [online]. Available at: Security-Issues-in-IoT_joa_Eng_0119.pdf.
Prasad, S.B., Madhumathy, P., 2021. Long term evolution for secured smart railway communications using internet of things. In: Machine Learning Algorithms for Industrial Applications. Springer, Cham, pp. 285–300.
PTC, 2018. The State of the Industrial Internet of Things: A Spotlight on Industrial Innovation. [online]. Available at: https://www.ptc.com/en/-/media/files/pdfs/iot/state-of-iot-whitepaper2.pdf?sc_lang=en.
Qi-cong, S.H.E.N., 2011. The Internet of Things Technology and Its Applications. *Logistics Engineering and Management*, *6*.
Ranjith, A., Vijayaragavan, S.P., 2020. Internet of Things (IoT) Based Automated Calamity Avoidance System for Railway Sectors. J. Comput. Theor. Nanosci. 17 (12), 5399–5408.
Ray, B.R., Abawajy, J., Chowdhury, M., 2014. Scalable RFID security framework and protocol supporting Internet of Things. Comput. Netw. 67, 89–103.
Rehman, H.U., Asif, M. and Ahmad, M., 2017, December. Future applications and research challenges of IOT. In *2017 International conference on information and communication technologies (ICICT)* (pp. 68-74). IEEE.

Rendon Schneir, J., Ajibulu, A., Konstantinou, K., Bradford, J., Zimmermann, G., Droste, H. and Canto, R., 2019. A business case for 5G mobile broadband in a dense urban area. *Telecommunications Policy*, *43*(7), pp.1-1.

Roman, R., Zhou, J., Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. 57 (10), 2266–2279.

Russom, P., 2011. Big data analytics. *TDWI best practices report, fourth quarter*, *19*(4), pp.1-34.

Safaeian, M., Fathollahi-Fard, A.M., Tian, G., Li, Z., Ke, H., 2019. A multi-objective supplier selection and order allocation through incremental discount in a fuzzy environment. J. Intell. Fuzzy Syst. 37 (1), 1435–1455.

Saghafi, F. and Kordsalari, H., 2018. Suggesting the Driving Forces behind the Effective Implementation of the Internet of Things in the IRI Railway System with Focus on Improving Safety. In *2018 9th International Symposium on Telecommunications (IST)* (pp. 375-380). IEEE.

Salah, K., Alfalasi, A., Alfalasi, M., Alharmoudi, M., Alzaabi, M., Alzyeodi, A. and Ahmad, R.W., 2020, January. IoT-enabled shipping container with environmental monitoring and location tracking. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-6). IEEE.

Saranya, C.M., Nitha, K.P., 2015. Analysis of Security methods in Internet of Things. Int. J. Recent Innovat. Trends Comput. Commun. 3 (4), 1970–1974.

Sarkar, C., SN, A.U.N., Prasad, R.V., Rahim, A., Neisse, R. and Baldini, G., 2015. DIAT: A scalable distributed architecture for IoT. *IEEE Internet of Things Journal*, *2*(3), pp.230-239.

Sayrafian, K., Yazdandoost, K.Y., 2015. Toward 5G Emerging Technologies: Selected Papers from IEEE PIMRC 2014. Int. J. Wireless Inf. Networks 22 (4), 295–297.

Seuring, S., Aman, S., Hettiarachchi, B.D., de Lima, F.A., Schilling, L., Sudusinghe, J.I., 2022. Reflecting on theory development in sustainable supply chain management. Cleaner Logistics and Supply Chain 3, 100016.

Shankar, T., Yamuna, G., Elanchezhian, E.B., 2019. Advanced landslide surveillance system for railway transport accident avoidance using Internet of Things (IoT). J. Comput. Theor. Nanosci. 16 (4), 1701–1705.

Sharma, A., Kaur, J., Singh, I., 2020. Internet of things (IoT) in pharmaceutical manufacturing, warehousing, and supply chain management. SN Computer Sci. 1 (4), 1–10.

Sharma, M.L., Kumar, S., Mehta, N., 2018. Internet of things application, challenges and future scope. Int. Res. J. Eng. Technol. (IRJET) 5 (2), 1376–1382.

Shi, L. and Wang, X.F., 2013. Design of Railway Information Platform Based on the Internet of Things. In *Advanced Materials Research* (Vol. 694, pp. 3345-3348). Trans Tech Publications Ltd.

Shoewu, O.O., Ayangbekun Oluwafemi, J., 2020. Insights into the development trends in 7G mobile wireless networks. J. Adv. Eng. Technol. 8 (1), 1–4.

Shu, Q., Zhong, S., Zeng, X., 2012. The Architecture of the Internet of Things in Railway Logistics. In: *ICLEM 2012: Logistics for Sustained Economic Development—Technology and Management for Efficiency*, pp. 1326–1332.

Singh, P., Dulebenets, M.A., Pasha, J., Gonzalez, E., Lau, Y., Kampmann, R., 2021a. Deployment of autonomous trains in rail transportation: current trends and existing challenges. IEEE Access 9, 91427–91461.

Singh, P., Pasha, J., Khorram-Manesh, A., Goniewicz, K., Roshani, A., Dulebenets, M.A., 2021b. A holistic analysis of train-vehicle accidents at highway-rail grade crossings in Florida. Sustainability 13 (16), 8842.

Singh, S., Sabde, K., Jais, R., Ukudde, A., Kshirsagar, P., Mohod, A., 2020. IoT based automatic vehicle detection for railway gates. Int. J. Res. Eng., Sci. Manage. 3 (7), 235–238.

SNCF, DB, Technische Universität Darmstadt and Télékom Paris, 2020. The internet of railway things security. [online]. Available at: https://www1.deutschebahn.com/resource/blob/5664326/57803c929dde6d12a3a206cf33421675/IoRT_Security-short-data.pdf.

Sneps-Sneppe, M. and Namiot, D., 2018. On 5G projects for urban railways. In *2018 22nd Conference of Open Innovations Association (FRUCT)* (pp. 244-249). IEEE.

Solanki, A. and Nayyar, A., 2019. Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In *Handbook of Research on Big Data and the IoT* (pp. 379-405). IGI Global.

Song, Y., 2013. Security in Internet of Things. Royal Institute of Technology. Master Thesis.

Spencer Jr, B.F., Park, J.W., Mechitov, K.A., Jo, H., Agha, G., 2017. Next generation wireless smart sensors toward sustainable civil infrastructure. Procedia Eng. 171, 5–13.

Staines R., 2018. Healthcare AI market worth $10bn plus by 2024-report. [online]. Available at: https://pharmaphorum.com/digital/healthcare-ai-market-worth-10bn-plus-2024-report/.

Statista.com, 2021. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030. [online]. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutorials 22 (2), 1191–1221.

Sun, Y., Qiang, H., Xu, J., Lin, G., 2020. Internet of Things-based online condition monitor and improved adaptive fuzzy control for a medium-low-speed maglev train system. IEEE Trans. Ind. Inf. 16 (4), 2629–2639.

Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., 2010. Vision and challenges for realizing the Internet of Things. Cluster of European research projects on the internet of things, European Commision 3 (3), 34–36.

Talpur, M.S.H., Sarwar, R., Oad, A., Buriro, H., Soomro, A.H., Luhrani, A., Rehman, H., Talpur, S.H., Chang, E.S., 2021. Smart Railway Track and Crossing Gate Security System Based on IoT. Int. J. Adv. Trends Comput. Sci. Eng. 10 (2), 1346–1355.

Tan, P., Wu, H., Li, P., Xu, H., 2018. Teaching management system with applications of RFID and IoT technology. Edu. Sci. 8 (1), 26.

Theophilus, O., Dulebenets, M.A., Pasha, J., Lau, Y.Y., Fathollahi-Fard, A.M., Mazaheri, A., 2021. Truck scheduling optimization at a cold-chain cross-docking terminal with product perishability considerations. Comput. Ind. Eng. 156, 107240.

Tyagi, H., Kumar, R., 2020. Cloud computing for IoT. In *Internet of Things (IoT)*. Springer, Cham, pp. 25–41.

Tzafestas, S.G., 2018. Ethics and law in the internet of things world. Smart Cities 1 (1), 98–120.

U.S. DOT, 2018. *AVs at Highway-Rail Grade Crossings-USDOT FRA final report*. [online]. Available: https://dotcms.fra.dot.gov/elibrary/automated-vehicles-highway-rail-grade-crossings-final-report.

U.S. DOT, 2021. *Automated Vehicles Comprehensive Plan*. [online]. Available: https://www.transportation.gov/av/avcp.

Udoh, I.S., Kotonya, G., 2018. Developing IoT applications: challenges and frameworks. IET Cyber-Phys. Syst.: Theor. Appl. 3 (2), 65–72.

Van Kranenburg, R., Bassi, A., 2012. IoT challenges. *Communications in Mobile*. Computing 1 (1), 1–5.

Verma, A., Shukla, V.K. and Sharma, R., 2021. Convergence of IOT in Tourism Industry: A Pragmatic Analysis. In *Journal of Physics: Conference Series* (Vol. 1714, No. 1, p. 012037). IOP Publishing.

Verma, G., Verma, H., 2021. A bibliometric content analysis for understanding 5G technology: promise, challenges and future road map. Inf. Technol. Ind. 9 (1), 254–261.

Verma, M., Bhardwaj, N., Yadav, A.K., 2016. Real time efficient scheduling algorithm for load balancing in fog computing environment. Int. J. Inf. Technol. Comput. Sci 8 (4), 1–10.

Virat, M.S., Bindu, S.M., Aishwarya, B., Dhanush, B.N. and Kounte, M.R., 2018. Security and privacy challenges in internet of things. In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 454-460). IEEE.

Virtanen, A., Silla, A., Jokela, M., Kauvo, K., 2019. Railroad level crossings and an autonomous vehicle. 13th ITS European Congress: Fulfilling ITS promises.

Voege, T., Godziejewski, B., Grand-Perret, S., Merat, N., Rødseth, Ø. and Schijndel-de Nooij, M., 2017. Connected and Automated Transport. [online]. Available: https://ec.europa.eu/.

Wahid, A., Kumar, P., 2015. A survey on attacks, challenges, and security mechanisms in wireless sensor network. Int. J. Innovat. Res. Sci. Technol. 1 (8), 189–196.

Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., Fu, C., 2010. Cloud computing: a perspective study. New Generation Computing 28 (2), 137–146.

Wang, Y., Sarkis, J., 2021. Emerging digitalisation technologies in freight transport and logistics: Current trends and future directions. Transp. Res. Part E 148, 102291.

Wazid, M., Das, A.K., Kumari, S., Khan, M.K., 2016. Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Security Commun. Networks 9 (17), 4596–4614.

F.P.J. Wester K. Krippendorff Content analysis An introduction to its methodology 2005 2005 9780761915447.

Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M.K., Choo, K.K.R., 2021. Consumer, commercial and industrial IoT (in) security: attack taxonomy and case studies. IEEE Internet Things J.

Xie, Z. and Qin, Y., 2019. High-speed railway perimeter intrusion detection approach based on Internet of Things. *Adv. Mech. Eng.*, *11*(2), p.1687814018821511.

Xu, R., Chen, Y., Blasch, E. and Chen, G., 2018. Blendcac: A blockchain-enabled decentralized capability-based access control for IoTs. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1027-1034). IEEE.

Yang, Z., Chen, M., Wong, K.K., Poor, H.V. and Cui, S., 2021. Federated learning for 6G: Applications, challenges, and opportunities. *arXiv preprint arXiv:2101.01338*.

Yi, D.L., Liang, D., 2010. A survey of the internet of things. Proc. of ICEBI 358–366.

Yi, S., Hao, Z., Qin, Z. and Li, Q., 2015, November. Fog computing: Platform and applications. In *2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb)* (pp. 73-78). IEEE.

Zantalis, F., Koulouras, G., Karabetsos, S., Kandris, D., 2019. A review of machine learning and IoT in smart transportation. Future Internet 11 (4), 94.

Zaouk, B. and Ozdemir, K., 2017, August. Implementing connected vehicle and autonomous vehicle technologies at highway-rail grade crossings. In *Grade Crossing Res. Needs Workshop* (Vol. 201, pp. 1-14).

Zarembski, A.M., 2014, October. Some examples of big data in railroad engineering. In *2014 IEEE International Conference on Big Data (Big Data)* (pp. 96-102). IEEE.

Zeinab, K.A.M., Elmustafa, S.A.A., 2017. Internet of things applications, challenges, and related future technologies. World Scientific News 2 (67), 126–148.

Zhang, J., Shao, L., 2013. An applied study on railway safety monitoring based on internet of things. J. Logistics, Inf. Serv. Sci. 1 (1), 1–11.

Zhang, R.X., Liu, Z.Y., Guo, J.W., 2011. Research on application of internet of things technology in railway transportation. J. Railway Eng. Soc. 10, 021.

Zhang, W., 2012. Study on internet of things application for high-speed train maintenance, repair, and operation (MRO). In *Proceedings of the National Conference on Information Technology and Computer Science (CITCS 2012), Lanzhou, China* (pp. 16-18).

Zhang, X., Kunz, A. and Schröder, S., 2017. Overview of 5G security in 3GPP. In *2017 IEEE conference on standards for communications and networking (CSCN)* (pp. 181-186). IEEE.

Zhao, K. and Ge, L., 2013, December. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security* (pp. 663-667). IEEE.

Zheng, Q., Wang, X., Khan, M.K., Zhang, W., Gupta, B.B., Guo, W., 2017. A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service. IEEE Access 6, 711–722.
Zhong, G., Xiong, K., Zhong, Z., Ai, B., 2021. Internet of things for high-speed railways. Intelligent Converged Networks 2 (2), 115–132.
Zhong, R.Y., Xu, X., Klotz, E., Newman, S.T., 2017. Intelligent manufacturing in the context of industry 4.0: a review. Engineering 3 (5), 616–630.
Zikria, Y.B., Ali, R., Afzal, M.K., Kim, S.W., 2021. Next-generation Internet of Things (IoT): opportunities, challenges, and solutions. Sensors 21 (4), 1174.