

Review

Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0

Robin Chataut ^{1,*}, , Alex Phoummalayvane ^{2,†} and Robert Akl ^{3,†}¹ School of Computing and Engineering, Quinnipiac University, Hamden, CT 06518, USA² Computer Science Department, Fitchburg State University, Fitchburg, MA 01420, USA; aphoumma@student.fitchburgstate.edu³ Department of Computer Science, University of North University, Denton, TX 76203, USA; robert.akl@unt.edu

* Correspondence: robin.chataut@quinnipiac.edu

† These authors contributed equally to this work.

Abstract: The Internet of Things (IoT) technology and devices represent an exciting field in computer science that is rapidly emerging worldwide. The demand for automation and efficiency has also been a contributing factor to the advancements in this technology. The proliferation of IoT devices coincides with advancements in wireless networking technologies, driven by the enhanced connectivity of the internet. Today, nearly any everyday object can be connected to the network, reflecting the growing demand for automation and efficiency. This paper reviews the emergence of IoT devices, analyzed their common applications, and explored the future prospects in this promising field of computer science. The examined applications encompass healthcare, agriculture, and smart cities. Although IoT technology exhibits similar deployment trends, this paper will explore different fields to discern the subtle nuances that exist among them. To comprehend the future of IoT, it is essential to comprehend the driving forces behind its advancements in various industries. By gaining a better understanding of the emergence of IoT devices, readers will develop insights into the factors that have propelled their growth and the conditions that led to technological advancements. Given the rapid pace at which IoT technology is advancing, this paper provides researchers with a deeper understanding of the factors that have brought us to this point and the ongoing efforts that are actively shaping the future of IoT. By offering a comprehensive analysis of the current landscape and potential future developments, this paper serves as a valuable resource to researchers seeking to contribute to and navigate the ever-evolving IoT ecosystem.

Keywords: IoT; smart cities; internet-of-medical-things; sensors; security; Industry 4.0

Citation: Chataut, R.; Phoummalayvane, A.; Akl, R. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. *Sensors* **2023**, *23*, 7194. <https://doi.org/10.3390/s23167194>

Academic Editor: Maurizio Mongelli

Received: 30 May 2023

Revised: 2 July 2023

Accepted: 4 July 2023

Published: 16 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things technology revolves around the core concept of integrating sensors into everyday objects and using connectivity to facilitate the exchange of information that is used in a variety of applications [1]. There are more everyday objects available than people, so the amount of connectivity that IoT devices hold is enormous [2]. In order to better understand the future of IoT technology, it is important to understand the unique circumstances that brought IoT to this point. A key distinction to make between the internet and the IoT is that the internet is a mesh of networks, whereas the IoT network is an interconnected network of devices [3,4]. An early example of the first IoT device was John Romkey's creation, which enabled a toaster to be turned on or off over the internet in 1990 [5]. It is clear that Internet of Things devices have come a long way from their humble beginnings, and there are many factors that influenced this rise. These devices play an important role in people's daily lives and involve the handling of massive amounts

of data [6]. IoT devices can be seen as a network of interconnected devices that involves sending and actuating devices that provide the ability to share information across different platforms [7–21].

The rapid rise in technology and computer system capabilities has had a major impact on the proliferation of Internet of Things (IoT) technology. The impact of IoT systems will impact many different fields and will change the way society operates and moves toward the future, as shown in Figure 1. This paper discusses the use of IoT in four domains. As IoT devices become increasingly integrated into society, there are still numerous security challenges that pose a threat to their spread. Numerous technologies are being developed in order to help protect the safe use of IoT devices, and it is clear that advances in security will be critical moving forward into the future [22–27].

Internet of Things

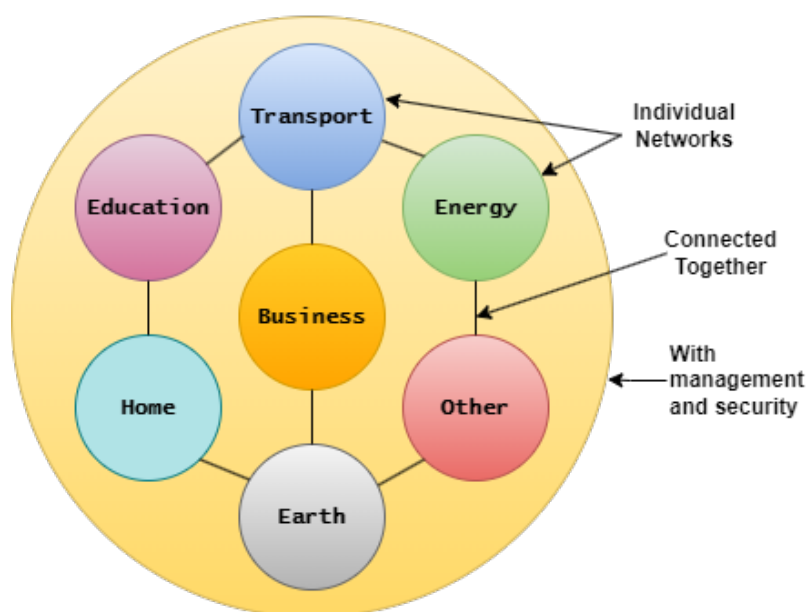


Figure 1. IoT technology and diverse application domains.

Numerous research works have been conducted to address various aspects of the Internet of Things (IoT), encompassing energy harvesting, device-to-device communication, energy efficiency, resource allocation, edge computing, security, privacy, and applications across different domains. Scholars have explored stochastic geometry analysis to optimize energy harvesting, proposed energy-efficient systems, investigated untapped potential in spectrum utilization, developed reinforcement learning-based frameworks, and explored the integration of edge computing and artificial intelligence [28–42]. Additionally, studies have focused on addressing security concerns in these areas, including privacy-preserving data sharing, explainable AI, and motion tracking. Collectively, these research efforts contribute to a comprehensive understanding of IoT technologies and their applications in diverse fields [43–51].

Many different strategies are being utilized by computing professionals in order to advance the field of research in IoT technology [52–56]. In particular, machine learning and artificial intelligence have played key roles in advancing this emerging field of computer science and will continue to do so in new and exciting ways [57]. It is critical for computer scientists to understand common machine learning and AI algorithms that are being used, as well as consider what research is currently being conducted to advance IoT technologies [58–73].

The methodology followed for conducting the review involves a systematic literature search, a study selection based on predefined criteria, data studies, a critical evaluation

of the selected studies, and a comprehensive discussion of the findings. This review aims to provide an overview of IoT applications and future directions in the selected domains, ensuring the inclusion of relevant research and a rigorous evaluation process.

2. Applications of IoT Devices

Since Internet of Things technology can be understood as devices/objects that are connected to a network, the applications of IoT devices are endless [74–80]. Leaders of different companies/organizations are recognizing the potential of IoT technology to make an impact and are investing more in these key pieces of technology in order to reap the benefits [81]. Nearly any object can be outfitted with the appropriate technology that will be involved in the data transmission from IoT devices and their connected networks. Writing about the different applications would be a long and arduous process and it would be more beneficial to first understand the most common applications of IoT devices before exploring what the future holds. Figures 2 and 3 shows growth in IoT globally. The connectivity in different medical IoT devices is shown in Figure 4.

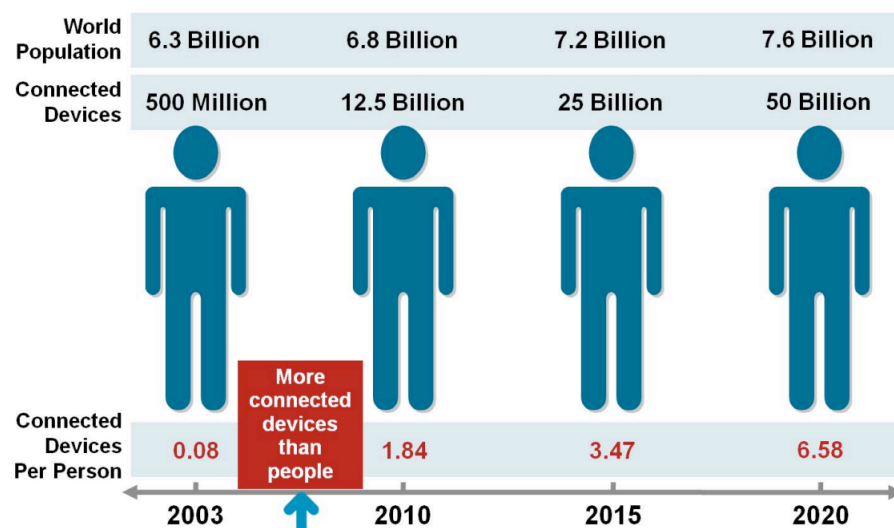


Figure 2. The number of IoT devices is greater than the number of people [82].

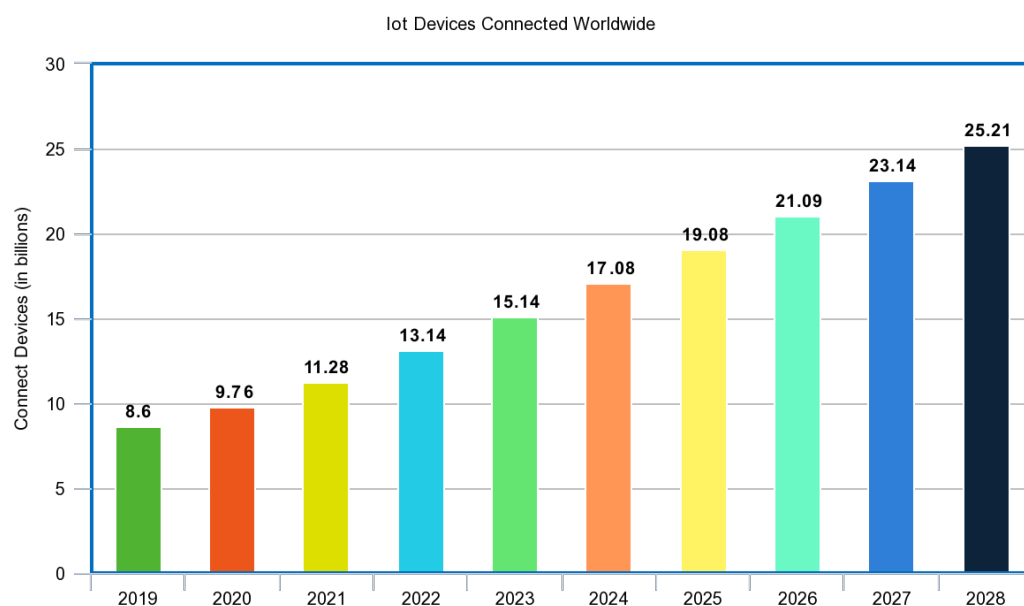


Figure 3. Number of IoT devices globally [83].






| Technology | Applications | Range |
|---|--|-------|
|  NB-IoT | Medical devices like glucose monitors, insulin pumps | Wide |
|  Bluetooth Low Energy | Wearable sensors | Low |
|  IEEE 802.11ax | Medical imaging, medical devices, streaming devices | Local |
|  IEEE 802.15.4 | Wearable sensors | Low |
|  5G Cellular | Wide range of applications | Wide |

Figure 4. Connectivity in different medical IoT devices.

2.1. Healthcare Applications

The Internet of Medical Things (IoTM) is an emerging subfield that is changing the way healthcare is being delivered through the use of IoT technology (Joyia). The use of IoT technology in healthcare has come a long way and continues to be a promising area for growth. Essential innovations, such as the AliveCor heart monitor, which relies on IoT sensors, show how useful technology can be when applied to healthcare in efforts to save lives [84]. Advances in technology have consistently played a major role in the healthcare industry, and IoT devices have found numerous applications in healthcare settings. One way that IoT devices are useful in healthcare is through the use of remote health monitoring in order to monitor patients at home rather than in hospitals [85]. The information that is collected from IoT devices is helpful in medical settings because it can be analyzed and used in ways such as early disease prediction [86]. IoT sensors even played a critical role during the COVID-19 pandemic in helping healthcare workers better monitor critical parameters that could save lives if changes were detected right away [87]. By examining these different IoT device applications in the healthcare industry, researchers can find additional ways to advance this field of research.

The use of sensors is critical in the delivery of healthcare services [88]. Sensors in medical devices act as a bridge between the physical and information worlds by collecting a variety of data. Sensors are crucial in helping healthcare professionals monitor different vitals that are important to measure in order to understand a person's health situation and act accordingly. Medical sensors can be used in a variety of ways in order to measure crucial information. Medical sensors are connected to IoT, and measure things such as temperature, respiration, heart rate, weight, skin conductance, galvanic response, blood flow/SpO₂, glucose testing, muscle contraction, and motion analysis [89]. The medical sensors are connected to wireless sensor networks, which relay useful information to different stakeholders involved in healthcare, such as patients, medical staff, insurers, and more [90]. The use of medical sensors is vast and can be used in crucial medical equipment, such as ECG monitors, glucose level sensing, and oxygen monitoring [91]. The goal of using any technology involved in healthcare is to promote better health outcomes, and IoT devices play a critical role in promoting this. Recent advances in IoT-related technology will continue to play a large role in creating stronger healthcare systems, and the future of healthcare will become increasingly reliant on technology [92].

Medical sensors are important in collecting useful information about a patient's health; however, this information is often very sensitive in nature, and this makes privacy a major concern moving forward. Security has always played a vital role in IoT technology; however, it matters even more in a situation such as healthcare, where IoT devices will be collecting sensitive information about patients that is private in nature [93]. If a patient's

medical information was compromised, this could lead to consequences for hospital organizations that did not employ the proper security measures to prevent it. The privacy and confidentiality of a patient's medical information are core concerns when addressing the security vulnerabilities of healthcare IoT devices [94].

There are many issues that present challenges to the successful use of IoT devices in healthcare and it is important to address these issues thoroughly when handling mission-critical operations, such as that of healthcare. Some important limitations that influence the use of IoT technology in medical devices include the need for high power consumption, the availability of limited resources, and handling security issues from the large number of devices being used [95].

The use of IoT technology in healthcare is promising and exciting. There are many useful applications where IoT devices can be used as sensors, and this helps healthcare providers in a variety of ways. Moving forward, IoT technology will continue to expand, and this will ultimately benefit healthcare organizations.

2.2. Agriculture Applications

As the population of the world grows at an exponential rate, the need for efficient food delivery systems is becoming a core issue that is a driver behind the advancements in smart agriculture [96]. In addition to the growing demand, factors such as climate change and water scarcity have also played roles in the increasing demand for more efficient agriculture systems [97]. Much of the technology around IoT implementation aims to reduce agricultural resource waste [98] as shown on Figure 5. The use of IoT technology in agricultural settings is critical to maintaining efficient operations and represents another common use case of IoT technology. Food supply chains that deliver quality and quantity are important to feed the world, and having efficient systems built around these supply chains will benefit people all over the world [99]. The need for more efficient food-delivery systems has helped to promote IoT use in agriculture because stakeholders saw the benefits that technology could provide [100].

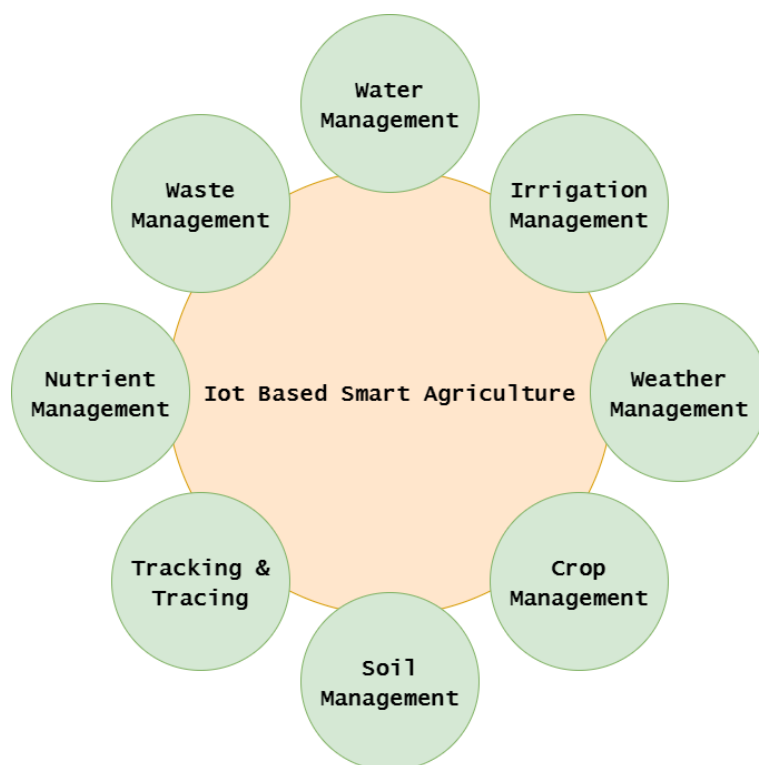


Figure 5. Different types of agriculture applications for IoT.

One way that IoT technology can be used in agriculture is automation. Automation involves having devices/objects respond automatically to different conditions without the need for human interaction. Wireless sensor networks are key proponents in helping IoT devices achieve their automation goals [101]. This can be useful in massive operations, such as agriculture, because of its sheer scale and need for efficient processes to maximize crop yields. For example, many sensors can be used in the soil of farmland in order to measure soil moisture content, in order to build systems that make better use of water for irrigation purposes [102]. These IoT devices can be used to measure soil conditions, such as water content, give appropriate signals when it is low, and turn on sprinkler systems automatically. Real-time monitoring and responses are very common and useful when understanding how IoT devices contribute to agriculture [103].

Data analytics is another area where IoT plays an important role in agriculture. Collecting and analyzing data are very useful because they can give important insight into how effective or ineffective an operation is. These data can be used to provide stakeholders with important insight that will ultimately impact their decision-making [104]. IoT devices collect massive amounts of data, and these data are useful when analyzed over time to help aid in decisions about estimation and forecasting [105]. The gathered data can be analyzed using machine learning methods that impact prediction, storage management, decision-making, farm management, and precision farming [96]. These data can become useful when attempting to implement more sustainable farming methods through the use of data-driven decision-making [104].

Although there is a large demand for efficient agriculture, there are other factors in play that have affected the proliferation of IoT devices in this sector. One key component that affects how widespread IoT devices are in agricultural applications is how costly it is to implement them in farming operations around the world [106]. Massive farming operations would require a large number of wireless sensors to collect data about a farming operation, and this can drastically increase the costs associated with implementing IoT in agriculture [107]. There are also many technical challenges that exist with implementing IoT technology in farms. Farms are often in large areas that are isolated and usually have poorer signals that impact their networking capabilities [108]. In addition to this, many farmers in rural parts of the world have limited knowledge of how to use IoT devices [109].

2.3. Smart Home Applications

Smart home applications represent promising use cases in which people benefit from IoT technology and there are numerous advantages/disadvantages to consider. Smart home devices date back to the 1970s when the X10 protocol was first conceived; this technology allowed for smart home devices to communicate properly [110]. IoT devices in smart homes can be used in a variety of ways, such as measuring home conditions, managing home appliances, and controlling home access [111]. Home automation remains a core feature around which IoT technology is applied [112]. For example, there are numerous home appliances that can be turned on and equipped with IoT technology in order to become more efficient and convenient [113]. There are many benefits that extend beyond convenience. The use of IoT sensors in smart homes can be used to assist the elderly in turning hard-to-reach devices on/off and even detect falls through the use of floor or camera sensors [114]. The market is being driven by the rising popularity of smart devices, such as speakers offered by Amazon and Google. According to a recently released report by Strategy Analytics, the global smart home market has had a positive outcome in recent years [115]. The report further estimates a compound annual growth rate (CAGR) of 10% from 2018 to 2023, leading to a market value of USD 155 billion, as shown in Figure 6.

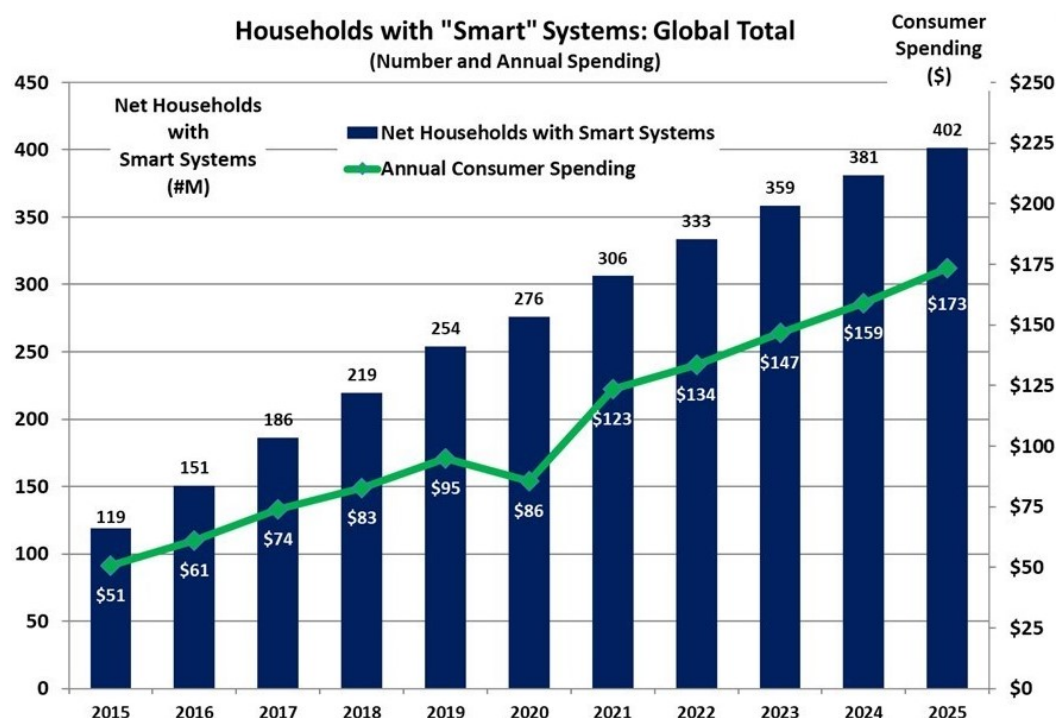


Figure 6. Households with smart systems: global total [115].

There are many techniques utilized in order to bring smart home technology to life. One important method relies on radio frequency identification (RFID) systems in order to act as enabler technologies for IoT [116]. RFID is an important technology that helps in identifying objects, recording data, and even controlling individual targets through the use of radio waves [117]. RFID devices can be used in a variety of ways. For example, higher education institutions can utilize RFID technology in student identification cards [118]. RFID technology is also used to detect the indoor roaming activity of elderly individuals and the data collected are used to provide more insight into the health of elderly individuals who live alone [119].

In an ideal future, IoT devices would be able to seamlessly communicate together [7]. There are many challenges that exist in the use of smart home IoT technology. Interoperability is one issue because the cost of using smart home technology is important to consider, and the integration of devices is a concern moving forward [120]. Different technologies utilized by IoT devices in order to create this connectivity include Wi-Fi, ZigBee, Z-Wave, Bluetooth LE, and Thread [121].

Security and privacy are also important to consider because smart grid technology can be a target for cyber attacks [120]. There are so many IoT objects that can be used in homes, and the dynamic and heterogeneous nature of smart home environments presents a challenge when it comes to addressing authentication and privacy issues [52]. Cyber attackers could target items such as smart home routers, gateways, or any other IoT-enabled devices to access data [122]. Many strategies are currently being analyzed in order to address smart home security needs. Blockchain is becoming increasingly utilized because of its benefits of having a decentralized database based on cryptographic techniques [55]. Although blockchain approaches have benefited from decentralized security/privacy, there are drawbacks when it comes to the energy and computational overhead that make it not ideal for IoT devices that are resource-constrained [123].

2.4. Smart Cities

Internet of Things devices have many useful applications when it comes to smart cities. A smart city can be understood as a city that is equipped with technology, such as wireless sensor networks and actuators that collect data; it is used to make important decisions in

city operations [124]. These systems are inherently complex due to the large number of devices, link layer technologies, and the different services involved in the operation of smart city technology [125]. The smart city concept consists of sensing networks, heterogeneous infrastructure, and information processing systems working together in order to improve a variety of areas within cities [126]. The use of IoT technology to enable smart cities is useful due to the quality of life it provides for the citizens within those cities [127]. The goal of smart cities is to use all of the information that is collected from IoT devices in order to improve the performances of urban services to citizens and also consider resource consumption at the same time [128].

Traffic monitoring is a very important application within the realm of smart cities. It is very common for metropolitan areas to be highly populated, and this causes congestion problems within these cities. Smart cities make use of information communication technologies in order to use the information to make decisions on how to dynamically handle traffic flow [129]. A smart traffic system (STS) involves real-time data collection and requires IoT devices to quickly obtain real-time public traffic data and have it processed [130]. The sensors used in smart traffic management systems can be embedded into roads in order to detect vehicles every 500 or 1000 meters [131]. Cameras are able to apply digital image processing techniques and, consequently, apply algorithms to aid in the prediction of traffic density; this information is then used accordingly [132]. Aside from helping traffic flow, smart traffic management systems also help with improving air quality and providing safety for the elderly [133].

Research indicates that the amount of solid waste will reach around 3.4 billion tons by the year 2050, and that will put a tremendous strain on municipal waste management systems [134]. Smart waste management is another growing application of IoT technology in smart cities. Nowadays, waste management systems are overtaxed and burdened due to the large demands of highly-populated urban areas [135]. The goal of smart waste management is to use IoT devices in order to optimize waste collection and reduce the negative impact on the environment [136]. Major factors driving the need for smart waste management include the demand for energy-efficient processes and the goal of creating healthier environments within cities [137]. A number of different objects can be repurposed into IoT devices, such as trash and recycling containers [138], and different technologies can be used to indicate when it is time to service a full container. In addition to detecting when waste bins are full, some sensors are capable of detecting unpleasant smells using gas sensors [139]. These smart containers essentially work by having sensors in the containers that read, collect, and communicate information about the amount of trash/recycle volume within them in order to better understand when it is time to empty the container [140].

In environmental sector applications, IoT technology has emerged as a valuable tool in enhancing air quality prediction through edge-based computation. Leveraging edge-based computation, IoT devices equipped with sensors collect real-time air quality data at the source, enabling precise prediction models tailored to specific locations. This empowers environmental monitoring systems to deliver accurate and timely information for effective decision-making and pollution control measures.

In the realm of anomaly detection and classification, IoT devices continuously monitor and analyze data from diverse sources, swiftly identify deviations from normal patterns, and recognize potential threats or irregularities. Through advanced machine learning algorithms and localized data processing, IoT systems can rapidly detect anomalies, ensuring the robust security and integrity of IoT networks and the data they generate.

Moreover, multisensory data fusion in multi-application wireless sensor data streams enables the integration of information from various sensors and applications, enabling a comprehensive understanding of intricate IoT environments. By combining data from disparate sources, such as temperature, humidity, and air quality sensors, IoT systems acquire a holistic view of the surroundings, generating valuable insights into informed decision-making across a wide range of applications, spanning from smart cities to industrial automation.

2.5. Industry 4.0

The manufacturing sector is undergoing a revolutionary transformation with the advent of Industry 4.0, ushering in an era of intelligent and interconnected systems. A prominent trend in this domain is the rapid adoption of Industrial Internet of Things (IIoT) devices and sensors [141–145] as shown in Figure 7. These embedded devices empower machines, equipment, and products to gather and transmit real-time data. The data generated by IIoT devices are invaluable for predictive maintenance, enabling manufacturers to proactively identify and address potential equipment failures, thereby reducing downtime and enhancing operational efficiency.

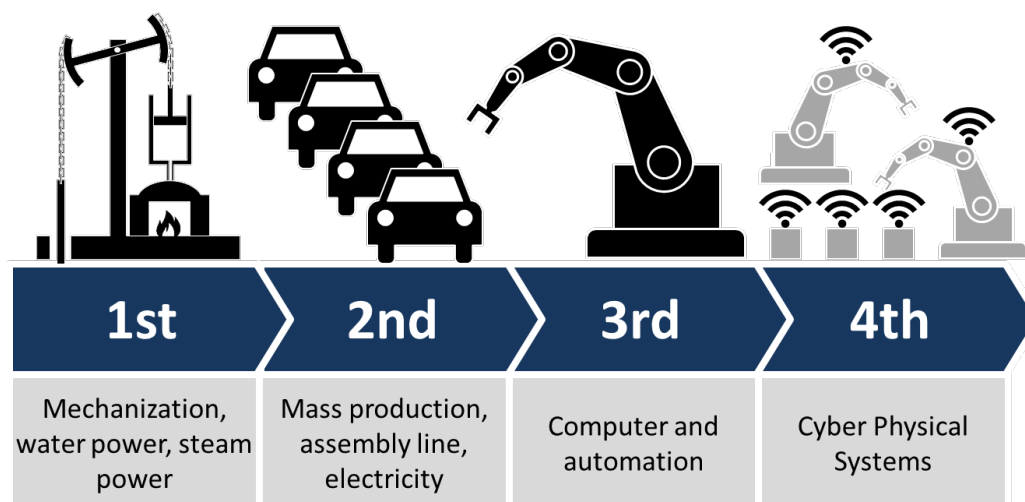


Figure 7. Industry 4.0.

Another significant trend within Industry 4.0 is the heightened focus on cybersecurity. As factories and supply chains become increasingly interconnected and reliant on digital technologies, the need for robust cybersecurity measures has become paramount. Manufacturers are making substantial investments in advanced security solutions to safeguard sensitive industrial data from cyber threats, ensuring the integrity and availability of their systems. This includes implementing encryption techniques, authentication protocols, and intrusion detection systems to fortify critical information.

Artificial intelligence (AI) and machine learning (ML) are also playing crucial roles in driving Industry 4.0 forward. With the copious amounts of data generated by IIoT devices, AI and ML algorithms have the capacity to analyze and derive meaningful insights from vast datasets. Manufacturers are leveraging these technologies to optimize production processes, enhance quality control, and improve decision-making. By detecting patterns and anomalies in real-time data, AI-powered systems can optimize manufacturing operations, identify defects, and propose process improvements, ultimately resulting in increased productivity and reduced costs.

Furthermore, the adoption of cloud computing technologies has empowered manufacturers to securely store and access vast quantities of data in a flexible and scalable manner. Cloud-based platforms provide the agility required for data analysis, collaboration, and remote monitoring. Manufacturers can conveniently access real-time production information from anywhere, enabling remote troubleshooting, predictive maintenance, and streamlined supply chain management.

Collaborative robots, also known as cobots, represent another noteworthy trend in Industry 4.0. These robots work alongside human operators, assisting them in various tasks and augmenting productivity. Cobots, which are designed to be safe, adaptable, and easily programmable, can adapt to changing production requirements. They are adept at handling repetitive and physically demanding tasks, freeing up human workers to concentrate on more intricate and creative aspects of the manufacturing process.

The integration of virtual reality (VR) and augmented reality (AR) technologies is also gaining momentum within Industry 4.0. These immersive technologies offer interactive and intuitive interfaces for training, simulation, and maintenance purposes. VR and AR enable workers to visualize and manipulate virtual representations of machinery, products, and processes, thereby enhancing training effectiveness and reducing errors.

Industry 4.0 is driving a transformative shift in the manufacturing landscape. The widespread adoption of IIoT devices, AI and ML algorithms, cloud computing, cybersecurity measures, cobots, and immersive technologies is reshaping traditional industrial processes into highly connected, intelligent, and efficient operations. Manufacturers who embrace these trends are poised to reap numerous benefits, including improved productivity, cost reductions, enhanced product quality, and increased agility in an intensely competitive global marketplace.

3. Challenges and Active Research Topics

3.1. Security of IoT Devices

The use of Internet of Things devices is progressively becoming more prevalent in the daily lives of people around the world; however, cyberattacks remain a large threat to the safe use of IoT [146]. Different examples of these devices are mobile phones, alarms, medical sensors, smartwatches, security systems, and more. The use of these devices continues to expand, and the need for strong security is vital to their success. Although these devices bring convenience, they come with many security issues and vulnerabilities. Since IoT devices often collect sensitive data, these data transmissions can be intercepted by third parties who intend to conduct harm or use these data for nefarious purposes. In one case, there were even attacks that could target IoT devices, such as the Mirai malware [147], which would hack/convert devices into its botnet and carry out DDoS attacks [148] as shown in Figure 8. Malware, such as the Mirai and others, take advantage of the vast amounts of poorly protected IoT devices, which commonly suffer from poor configurations and open designs, making them targets [149]. Detecting malware and IoT botnets remains an active research area, and many techniques are being applied. The use of a lightweight approach in the classification of IoT malware through the use of image recognition is just one example [150]. Other ways include the use of machine learning algorithms that use supervised, unsupervised, and reinforcement learning in order to handle tasks such as authentication, access control, and malware detection [151].

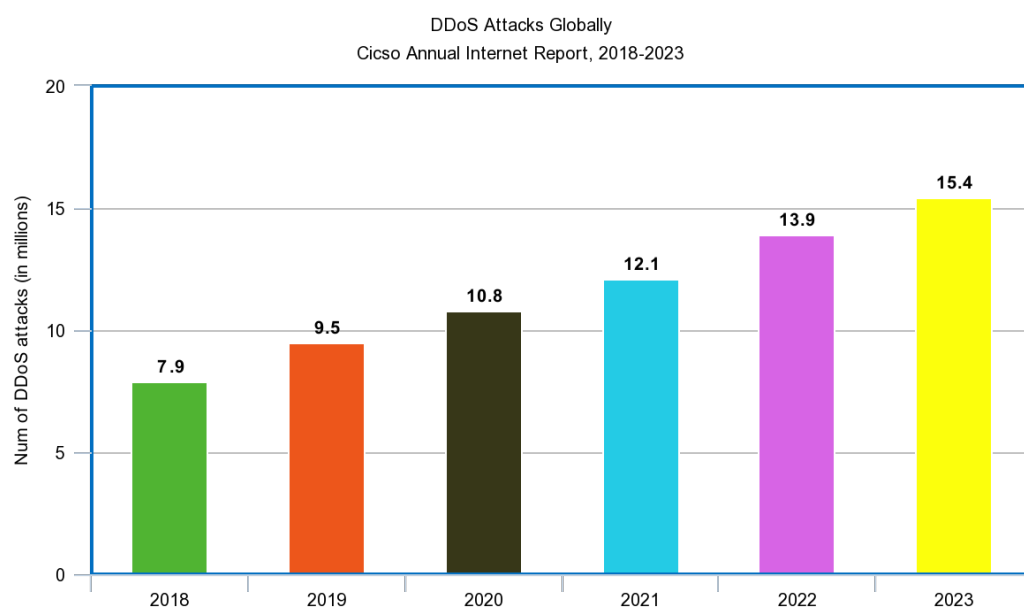


Figure 8. DDoS attacks worldwide.

There is an enormous amount of data being transmitted on a daily basis, which impacts critical operations across many applications. It could be possible for attackers to disrupt entire networks that rely on IoT technology, and the consequences would be devastating [152]. Hackers and criminals could seriously impact the expansion of IoT devices in the future, and it is crucial that security be thoroughly researched to mitigate these negative impacts.

3.2. Authentication and Password Security

One security issue is the lack of security in regard to authentication and passwords. Many IoT devices rely on password security in order to stay protected from cyber criminals who are attempting to gain access to them. These passwords can often be weak, and criminals can have easy access to IoT devices. There is a lack of standardization revolving around how complex passwords should be. Research shows that having more complex password combinations in IoT devices can prevent more cyber attacks [153]. Even with stronger passwords, there would need to be additional security measures to prevent cyber attackers.

One example of an additional layer of security involves the use of multi-authentication in IoT devices. In order to authorize the correct users to access IoT devices, it is a prerequisite to first have authentication [154]. Authentication is the process by which the identity of users is verified before allowing them to gain access to a system. Passwords represent just one level of authentication, and it is important to understand the other types of authentication mechanisms that IoT devices can take advantage of. Different methods, such as the utilization of elliptic curve cryptography, can be useful when performing authentications in IoT security systems [155].

One-time passwords can sometimes be useful for authentication purposes related to IoT devices. These passwords work by having a private key generator (PKG) generate a one-time password, and this password is used as a private key that is needed in order to gain access. The last phase of using one-time passwords involves validation. In this phase, the application and IoT device exchange data via a one-time password, verifying that the password was sourced from a valid location [156].

3.3. Interoperability Challenges

Using IoT devices smoothly and without compatibility issues remains a challenge both now and in the future. Interoperability is important because it allows IoT devices to communicate with each other more efficiently. It is a challenge to have IoT devices work together seamlessly because many operate on different infrastructures, devices, APIs, and even data formats [156]. The need for the safe interoperability of IoT devices has even led to the creation of international organizations that develop standards that IoT devices can adopt with the intention of becoming more compatible [157]. The use of protocols and standards, such as Bluetooth and ZigBee, is critical to the rise of IoT technology because it essentially establishes the rules for use and communication, helping to address interoperability concerns [158]. International organizations, such as IEEE, the Internet Engineering Task Force (IETF), OneM2M, and others, have developed important standards and protocols and play integral roles in influencing the IoT [159]. One important contribution to addressing these challenges is the BiG IoT project, which is an initiative that seeks to create a common API that different IoT devices could communicate through [160].

3.4. Cloud Computing Research

Since IoT devices generate massive amounts of data, cloud computing solutions are continually being used and researched in order to better handle these data demands. Cloud IoT is a novel IT paradigm that represents the merging of the cloud with IoT, and research in this area will be crucial in moving this technology forward [161]. Cloud computing is essentially an extension of distributed computing, parallel computing, and grid computing [126]. There are many IoT constraints that cloud computing addresses,

such as processing, storage, and communication [162]. For example, a major concern about IoT data involves the security risks that come from storing data locally on IoT devices [163], and cloud computing aims to address this concern by allowing data storage in cloud computing servers [164]. Since data collected from IoT devices are often unstructured, cloud computing research looks to improve the real-time data processing capabilities and allow for more dynamic resource management [165].

3.5. Potential Future Directions and Developments

The potential future directions and developments of IoT in healthcare, agriculture, smart homes, smart cities, and Industry 4.0 are poised to bring about transformative changes and advancements. In healthcare, the integration of IoT with telemedicine, wearable health technology, and advanced data analytics holds promise for revolutionizing patient care. Real-time monitoring, personalized treatment plans, and early disease detection can be facilitated through IoT-enabled devices, leading to improved health outcomes. In agriculture, IoT-driven precision farming techniques, such as smart irrigation and crop disease detection, have the potential to optimize resource utilization, conserve water, and enhance crop yield. By leveraging real-time data from IoT sensors, farmers can make informed decisions and implement timely interventions. In the realm of smart homes, the focus will be on seamless integration, energy efficiency, and personalized automation. IoT-enabled smart home solutions will allow for centralized control and management of various devices, optimizing energy consumption and providing tailored experiences for inhabitants. In smart cities, IoT applications will enhance transportation systems, environmental monitoring, and citizen engagement. Intelligent traffic management, real-time tracking of air quality, and participatory governance will contribute to improved mobility, sustainability, and quality of life. Finally, Industry 4.0 will witness the integration of IoT in industrial automation, predictive maintenance, and supply chain optimization. IoT-driven technologies will enable the real-time monitoring of machines, predictive maintenance strategies, and streamlined logistics, leading to enhanced productivity and reduced downtime. Continued research and development in these areas will shape the future of IoT, paving the way for innovative solutions and transformative advancements across sectors.

4. Conclusions

IoT technology has rapidly emerged as a revolutionary field in computer science, facilitating the connection of everyday objects to the internet and enabling a vast network of interconnected devices. The widespread adoption of IoT devices has been fueled by advancements in wireless networking technologies and the increasing demand for automation and efficiency across multiple industries. This technology is being utilized across various sectors, and its utilization is expected to continue expanding. IoT is progressively integrating into society and has become particularly significant in areas such as healthcare, agriculture, smart homes, smart cities, and more. The progress in technological and networking capabilities underscores the pivotal role of emerging technologies in driving the proliferation of IoT worldwide. However, despite its potential, there are several challenges, including security and privacy concerns, which researchers must address through innovative approaches. As networking and technological advancements continue to support the rise of IoT, its applications will further grow and become increasingly integrated into our societal fabric. This paper has examined the emergence of IoT devices, explored their common applications in healthcare, agriculture, and smart cities, and delved into the future prospects of this promising field.

The future of IoT technology holds tremendous promise. Advancements in machine learning and artificial intelligence will play vital roles in driving innovation in this field, unlocking new possibilities for IoT applications. However, it is essential to tackle security challenges, enhance affordability, and raise awareness and knowledge among users and stakeholders to ensure the sustained growth and success of IoT technology.

To summarize, IoT technology has brought about a revolution in various industries, offering vast opportunities for automation, efficiency, and improved decision-making. By comprehending the driving forces behind the emergence of IoT devices and exploring their applications in different fields, researchers and practitioners can shape the future of IoT and harness its potential for the betterment of society.

Author Contributions: Conceptualization, R.C., A.P. and R.A.; methodology, R.C., A.P. and R.A.; writing—original draft preparation, R.C., A.P. and R.A.; writing—review and editing, R.C., A.P. and R.A. The authors declare that they have equally contributed to the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank the authors of the literature cited in this paper for contributing the useful ideas to this study.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

| | |
|------|---------------------------------|
| IoT | Internet of Things |
| IoMT | Internet of Medical Things |
| DDOS | distributed denial of service |
| RFID | radio frequency identification |
| STS | smart traffic systems |
| PKG | private key generator |
| IETF | Internet Engineering Task Force |

References

1. Saleem, S.I.; Zeebaree, S.; Zeebaree, D.Q.; Abdulazeez, A.M. Building smart cities applications based on IoT technologies: A review. *Technol. Rep. Kansai Univ.* **2020**, *62*, 1083–1092.
2. Said, O.; Masud, M. Towards internet of things: Survey and future vision. *Int. J. Comput. Netw.* **2013**, *5*, 1–17.
3. Paul, C.; Ganesh, A.; Sunitha, C. An overview of IoT based smart homes. In Proceedings of the 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 43–46.
4. Tan, L.; Wang, N. Future Internet: The Internet of Things. In Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering, ICACTE 2010, Chengdu, China, 20–22 August 2010; pp. V5-376–V5-380.
5. Suresh, P.; Daniel, J.V.; Parthasarathy, V.; Aswathy, R.H. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In Proceedings of the 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, India, 27–29 November 2014; pp. 1–8.
6. Al-Khafajiy, M.; Webster, L.; Baker, T.; Waraich, A. Towards fog driven IoT healthcare: Challenges and framework of fog computing in healthcare. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, 26–27 June 2018; pp. 1–7.
7. Alaa, M.; Zaidan, A.A.; Zaidan, B.B.; Talal, M.; Kiah, M.L.M. A review of smart home applications based on Internet of Things. *J. Netw. Comput. Appl.* **2017**, *97*, 48–65. [[CrossRef](#)]
8. Sharma, S.; Kaushik, B. A survey on Internet of vehicles: Applications, security issues and solutions. *Veh. Commun.* **2019**, *20*, 100182.
9. Silva, C.; Silva, F.; Sarubbi, J.; Oliveira, T.; Meira, W.; Nogueira, J. Designing mobile content delivery networks for the Internet of vehicles. *Veh. Commun.* **2017**, *8*, 45–55. [[CrossRef](#)]
10. Lei, T.; Wang, S.; Li, J.; Yang, F. A cooperative route choice approach via virtual vehicle in iov. *Veh. Commun.* **2017**, *9*, 281–282. [[CrossRef](#)]
11. Bajaj, R.; Rao, M.; Agrawal, H. Internet of things (IoT) in the smart automotive sector: A review. *IOSR J. Comput. Eng.* **2018**, *9*, 36–44.

12. Ganesh, E.N. Implementation of IoT architecture for SMART HOME using GSM technology. *Int. J. Comput. Tech.* **2017**, *4*, 42–48.
13. Shafique, K.; Khawaja, B.A.; Sabir, F.; Qazi, S.; Mustaqim, M. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access* **2020**, *8*, 23022–23040. [[CrossRef](#)]
14. Ahmadi, H.; Arji, G.; Shahmoradi, L.; Safdari, R.; Nilashi, M.; Alizadeh, M. The application of internet of things in healthcare: A systematic literature review and classification. *Univers. Access Inf. Soc.* **2019**, *18*, 837–869. [[CrossRef](#)]
15. Ahad, A.; Tahir, M.; Yau, K.A. 5g-based smart healthcare network: Architecture, taxonomy, challenges and future research directions. *IEEE Access* **2019**, *7*, 100747–100762. [[CrossRef](#)]
16. Ramachandran, A.; Pahwa, P.K.R.A. Machine learning-based techniques for fall detection in geriatric healthcare systems. In Proceedings of the 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, China, 19–21 October 2018; pp. 232–237.
17. Shaikh, Y.; Parvati, V.K.; Biradar, S.R. Survey of smart healthcare systems using internet of things (IoT): (invited paper). In Proceedings of the 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 15–17 February 2018; pp. 508–513.
18. Rajini, N.H. A comprehensive survey on internet of things based healthcare services and its applications. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 483–488.
19. Song, X.; Chin, K.-W. Maximizing Packets Collection in Wireless Powered IoT Networks with Charge-or-Data Time Slots. *IEEE Trans. Cogn. Commun. Netw.* **2023**, *9*, 1067–1079. [[CrossRef](#)]
20. Liu, X.; Xu, B.; Wang, X.; Zheng, K.; Chi, K.; Tian, X. Impacts of Sensing Energy and Data Availability on Throughput of Energy Harvesting Cognitive Radio Networks. *IEEE Trans. Veh. Technol.* **2023**, *72*, 747–759. [[CrossRef](#)]
21. Vishwakarma, S.K.; Upadhyaya, P.; Kumari, B.; Mishra, A.K. Smart Energy Efficient Home Automation System Using IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–4.
22. Tan, J.; Sha, X.; Lu, T.; Dai, B. A Short Survey on Future Research of AI and IoT Technologies. In Proceedings of the 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 30 May–3 June 2022; pp. 190–195.
23. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies, and Future Directions. *Sensors* **2023**, *23*, 1805. [[CrossRef](#)] [[PubMed](#)]
24. Chataut, R.; Akl, R. Massive MIMO Systems for 5G and beyond Networks—Overview, Recent Trends, Challenges, and Future Research Direction. *Sensors* **2020**, *20*, 2753. [[CrossRef](#)]
25. Affia, A.-A.O.; Finch, H.; Jung, W.; Samori, I.A.; Potter, L.; Palmer, X.-L. IoT Health Devices: Exploring Security Risks in the Connected Landscape. *IoT* **2023**, *4*, 150–182. [[CrossRef](#)]
26. Tang, S. Performance Modeling and Optimization for a Fog-Based IoT Platform. *IoT* **2023**, *4*, 183–201. [[CrossRef](#)]
27. Nayernia, H.; Papagiannidis, H.B.S. A systematic review of the implementation of industry 4.0 from the organisational perspective. *Int. J. Prod. Res.* **2022**, *60*, 4365–4396. [[CrossRef](#)]
28. Chu, M.; Liu, A.; Chen, J.; Lau, V.K.N.; Cui, S. A Stochastic Geometry Analysis for Energy-Harvesting-Based Device-to-Device Communication. *IEEE Internet Things J.* **2022**, *9*, 1591–1607. [[CrossRef](#)]
29. Almasoud, A.M.; Alsharoa, A.; Qiao, D.; Kamal, A.E. An Energy-Efficient Internet of Things Relaying System for Delay-Constrained Applications. *IEEE Access* **2022**, *10*, 82259–82271. [[CrossRef](#)]
30. Fernandes, V.; Cravo, N.; Monteiro, H.L.M.; Jayakody, D.N.K.; Poor, H.V.; Ribeiro, M.V. Energy Harvesting in the UNB-PLC Spectrum: Hidden Opportunities for IoT Devices. *IEEE Internet Things J.* **2023**, *10*, 1236–1247. [[CrossRef](#)]
31. Zheng, K.; Jia, X.; Chi, K.; Liu, X. DDPG-Based Joint Time and Energy Management in Ambient Backscatter-Assisted Hybrid Underlay CRNs. *IEEE Trans. Commun.* **2023**, *71*, 441–456. [[CrossRef](#)]
32. Wang, X.; Zhang, Y.; Shen, R.; Xu, Y.; Zheng, F.-C. DRL-Based Energy-Efficient Resource Allocation Frameworks for Uplink NOMA Systems. *IEEE Internet Things J.* **2020**, *7*, 7279–7294. [[CrossRef](#)]
33. Nguyen, N.-T.; Nguyen, D.N.; Hoang, D.T.; Van Huynh, N.; Dutkiewicz, E.; Nguyen, N.-H.; Nguyen, Q.-T. Time Scheduling and Energy Trading for Heterogeneous Wireless-Powered and Backscattering-Based IoT Networks. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 6835–6851. [[CrossRef](#)]
34. Nguyen, N.-T.; Nguyen, D.N.; Hoang, D.T.; Van Huynh, N.; Nguyen, H.-N.; Nguyen, Q.T.; Dutkiewicz, E. Energy Trading and Time Scheduling for Energy-Efficient Heterogeneous Low-Power IoT Networks. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
35. Guo, W.; Jing, L. Towards Low-Cost Passive Motion Tracking with One Pair of Commodity Wi-Fi Devices. *IEEE J. Indoor Seamless Position Navig.* **2023**, *1*, 39–52. [[CrossRef](#)]
36. Zhang, S.; Liu, A.; Han, C.; Liang, X.; Xu, X.; Wang, G. Multi-agent Reinforcement Learning-Based Orbital Edge Offloading in SAGIN Supporting Internet of Remote Things. *IEEE Internet Things J.* **2023**. [[CrossRef](#)]
37. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [[CrossRef](#)]
38. McEnroe, P.; Wang, S.; Liyanage, M. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. *IEEE Internet Things J.* **2022**, *9*, 15435–15459. [[CrossRef](#)]

39. Liu, J.; Fan, Y.; Sun, R.; Liu, L.; Wu, C.; Mumtaz, S. Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System. *IEEE Internet Things J.* **2023**. [\[CrossRef\]](#)
40. Kok, İ.; Okay, F.Y.; Muyanli, O.; Ozdemir, S. Explainable Artificial Intelligence (XAI) for Internet of Things: A Survey. *IEEE Internet Things J.* **2023**, *10*, 14764–14779. [\[CrossRef\]](#)
41. Rice, M.; Kirkwood, R.; Landon, L.; Walker, P.; Harrison, W. On Polarization Diversity in 5G and Beyond Internet-of-Things Networks. In Proceedings of the 2023 Intermountain Engineering, Technology and Computing (IETC), Provo, UT, USA, 12–13 May 2023; pp. 126–131.
42. Chen, S.; Xu, H.; Liu, D.; Hu, B.; Wang, H. A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective. *IEEE Internet Things J.* **2014**, *1*, 349–359. [\[CrossRef\]](#)
43. Yaklaf, S.K.A.; Elmezughi, A.S.; Naas, S.M.H.; Ekreem, N.B. Privacy, Security, Trust and Applications in Internet of Things. In Proceedings of the 2023 IEEE International Conference on Advanced Systems and Emergent Technologies (ICASET), Hammamet, Tunisia, 29 April–1 May 2023; pp. 1–6.
44. HChi, R.; Radwan, A. Quality of Things' Experience for 6G Artificial Intelligent Internet of Things with IEEE P2668. *IEEE Commun. Mag.* **2023**, *61*, 58–64.
45. Jung, S.; Jeong, S.; Kang, J.; Kang, J. Marine IoT Systems with Space-Air-Sea Integrated Networks: Hybrid LEO and UAV Edge Computing. *IEEE Internet Things J.* **2023**. [\[CrossRef\]](#)
46. Qiu, S.; Wei, Z.; Huang, Y.; Abbaszadeh, M.; Charmet, J.; Li, B.; Guo, W. Review of Physical Layer Security in Molecular Internet of Nano-Things. *IEEE Trans. Nanobioscience* **2023**, *Online ahead of print*. [\[CrossRef\]](#)
47. Yin, Y.; Di, Q.; Wan, J.; Liang, T. Time-Aware Smart City Services based on QoS Prediction: A Contrastive Learning Approach. *IEEE Internet Things J.* **2023**. [\[CrossRef\]](#)
48. Ashraf, Q.M.; Tahir, M.; Habaebi, M.H.; Isoaho, J. Toward Autonomic Internet of Things: Recent Advances, Evaluation Criteria, and Future Research Directions. *IEEE Internet Things J.* **2023**, *10*, 14725–14748. [\[CrossRef\]](#)
49. Li, X.; Hu, X.; Jiang, T. Dual Reinforcement Learning based Attack Path Prediction for 5G Industrial Cyber-Physical Systems. *IEEE Internet Things J.* **2023**. [\[CrossRef\]](#)
50. Andhare, M.S.; Kumbhar, V.S.; Tekade, A.A. Detecting Cybersecurity Attacks in Industrial Internet of Things: A Systematic Literature Review. In Proceedings of the 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 20–21 January 2023; pp. 1–7.
51. Goyal, H.R.; Sharma, S. Flood Management System Using Cloud Computing and Internet-of-Things. In Proceedings of the 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 20–21 January 2023; pp. 1–6.
52. Ali, T.; Irfan, M.; Alwadie, A.S.; Glowacz, A. IoT-based smart waste bin monitoring and municipal solid waste management system for smart cities. *Arab. J. Sci. Eng.* **2020**, *45*, 10185–10198. [\[CrossRef\]](#)
53. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based smart home: Security challenges, security requirements, and solutions. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
54. Alotaibi, M. Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN. *IEEE Access* **2021**, *9*, 159187–159197. [\[CrossRef\]](#)
55. Arif, S.; Khan, M.A.; Rehman, S.U.; Kabir, M.A.; Imran, M. Investigating smart home security: Is blockchain the answer? *IEEE Access* **2020**, *8*, 117802–117816. [\[CrossRef\]](#)
56. Atwady, Y.; Hammoudeh, M. A survey on authentication techniques for the internet of things. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017.
57. Morgan, J.; Lu, M. What Is Internet of Things? IoT For All. Available online: <https://www.iotforall.com/what-is-internet-of-things> (accessed on 1 July 2023).
58. Din, U.D.; Bano, A.; Awan, K.A.; Almogren, A.; Altameem, A.; Guizani, M. LightTrust: Lightweight trust management for edge devices in industrial Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 2776–2783. [\[CrossRef\]](#)
59. Rui, L.; Yang, S.; Gao, Z.; Li, W.; Qiu, X.; Meng, L. Smart network maintenance in edge cloud computing environment: An allocation mechanism based on comprehensive reputation and regional prediction model. *J. Netw. Comput. Appl.* **2022**, *198*, 103298. [\[CrossRef\]](#)
60. Kumar, V.; Mahmoud, M.S.; Alkhayyat, A.; Srinivas, J.; Kumari, M.A.A. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcar infrastructure. *J. Supercomput.* **2022**, *78*, 6167–6196. [\[CrossRef\]](#)
61. Van Geest, M.; Tekinerdogan, B.; Catal, C. Smart Warehouses: Rationale, Challenges and Solution Directions. *Appl. Sci.* **2022**, *12*, 219. [\[CrossRef\]](#)
62. Guan, Z.; Wang, Y.; He, M. Deep Reinforcement Learning-Based Spectrum Allocation Algorithm in Internet of Vehicles Discriminating Services. *Appl. Sci.* **2022**, *12*, 1764. [\[CrossRef\]](#)
63. Singh, P.; Kaur, A.; Batth, R.S.; Aujla, G.S.; Masud, M. Service Versus Protection: A Bayesian learning approach for trust provisioning in edge of things environment. *IEEE Internet Things J.* **2022**, *9*, 22061–22070. [\[CrossRef\]](#)
64. Dinesh, G.; Pawar, Y.S.; Dinshi, P.; S, S.; Husain, S.S.; Reddy, C.V.K. Machine Learning based Secure Data Transmission and Improvement in MANET through Internet of Things (IoT). In Proceedings of the 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 5–7 January 2023; pp. 1006–1012.

65. Wu, Y.-J.; Brito, R.; Choi, W.-H.; Lam, C.-S.; Wong, M.-C.; Sin, S.-W.; Martins, R.P. IoT Cloud-Edge Reconfigurable Mixed-Signal Smart Meter Platform for Arc Fault Detection. *IEEE Internet Things J.* **2023**, *10*, 1682–1695. [\[CrossRef\]](#)
66. Islam, M.M.; Nooruddin, S.; Karray, F.; Muhammad, G. Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain. *IEEE Internet Things J.* **2023**, *10*, 3611–3641. [\[CrossRef\]](#)
67. Nataraj, P.K.B.; Duraisamy, P. An Investigation on Attacks in Application Layer Protocols and Ransomware Threats in Internet of Things. In Proceedings of the 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 17–18 March 2023; pp. 668–672.
68. Joel, M.R.; Manikandan, G.; Bhuvaneswari, G. An Analysis of Security Challenges in Internet of Things (IoT) based Smart Homes. In Proceedings of the 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2–4 March 2023; pp. 490–497.
69. Celik, A.; Romdhane, I.; Kaddoum, G.; Eltawil, A.M. A Top-Down Survey on Optical Wireless Communications for the Internet of Things. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 1–45. [\[CrossRef\]](#)
70. Ullah, R.; Asghar, I.; Griffiths, M.G.; Stacey, C.; Stiles, W.; Whitelaw, C. Internet of Things based Sensor System for Vertical Farming and Controlled Environment Agriculture. In Proceedings of the 2023 6th Conference on Cloud and Internet of Things (CIoT), Lisbon, Portugal, 20–22 March 2023; pp. 136–140.
71. Chataut, R.; Akl, R.; Dey, U.K.; Robaei, M. SSOR Preconditioned Gauss-Seidel Detection and Its Hardware Architecture for 5G and beyond Massive MIMO Networks. *Electronics* **2021**, *10*, 578. [\[CrossRef\]](#)
72. Soni, T.; Gupta, D.; Uppal, M. Bibliometric Analysis on Security of Different Layers in Internet of Things (IoT) Environment. In Proceedings of the 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 1–3 March 2023; pp. 1–6.
73. Karpagam, M. Smart Energy Meter and Monitoring System using Internet of Things (IoT). In Proceedings of the 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 5–7 January 2023; pp. 75–80.
74. Chen, W.E.; Wang, Y.H.; Huang, P.C.; Huang, Y.Y.; Tsai, M.Y. A smart IoT system for waste management. In Proceedings of the 2018 1st International Cognitive Cities Conference (IC3), Okinawa, Japan, 7–9 August 2018; pp. 202–203.
75. Durga, S.; Nag, R.; Daniel, E. Survey on machine learning and deep learning algorithms used in internet of things (IoT) healthcare. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 1018–1022.
76. Hsu, H.-T.; Jong, G.-J.; Chen, J.-H.; Jhe, C.-G. Improve Iot Security System of Smart-Home by Using Support Vector Machine. In Proceedings of the 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 23–25 February 2019.
77. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1686–1721. [\[CrossRef\]](#)
78. Joyia, G.J.; Liaqat, R.M.; Farooq, A.; Rehman, S. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* **2017**, *12*, 240–247. [\[CrossRef\]](#)
79. Ojha, T.; Misra, S.; Raghuwanshi, N.S. Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Comput. Electron. Agric.* **2015**, *118*, 66–84. [\[CrossRef\]](#)
80. Zhang, S.; Zhang, S.; Chen, X.; Huo, X. Cloud computing research and development trend. In Proceedings of the 2010 Second International Conference on Future Networks, Washington, DC, USA, 22–24 January 2010; pp. 93–97.
81. Pardini, K.; Rodrigues, J.J.; Diallo, O.; Das, A.K.; de Albuquerque, V.H.C.; Kozlov, S.A. A smart waste management solution geared towards citizens. *Sensors* **2020**, *20*, 2380. [\[CrossRef\]](#) [\[PubMed\]](#)
82. Evans, D. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*; Cisco Internet Business Solutions Group (IBSG): San Jose, CA, USA, 2011.
83. Transforma Insights, Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2021, with Forecasts from 2022 to 2030 (in Billions). Statista. Available online: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (accessed on 14 June 2023).
84. Halcox, J.P.; Wareham, K.; Cardew, A.; Gilmore, M.; Barry, J.P.; Phillips, C.; Gravenor, M.B. Assessment of remote heart rhythm sampling using the AliveCor heart monitor to screen for atrial fibrillation: The REHEARSE-AF study. *Circulation* **2017**, *136*, 1784–1794. [\[CrossRef\]](#)
85. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [\[CrossRef\]](#)
86. Khan, M.A. Challenges facing the application of IoT in medicine and healthcare. *Int. J. Comput. Inf. Manuf. (IJCIM)* **2021**, *1*, 39–55. [\[CrossRef\]](#)
87. Javaid, M.; Khan, I.H. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofacial Res.* **2021**, *11*, 209–214. [\[CrossRef\]](#)
88. Shah, S.T.U.; Yar, H.; Khan, I.; Ikram, M.; Khan, H. Internet of things-based healthcare: Recent advances and challenges. *Appl. Intell. Technol. Healthc.* **2019**, 153–162. [\[CrossRef\]](#)
89. Yuehong, Y.I.N.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13.

90. Maksimović, M.; Vujović, V.; Perišić, B. A custom Internet of Things healthcare system. In Proceedings of the 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, Portugal, 7–20 June 2015; pp. 1–6.
91. Tekeste Habte, T.; Saleh, H.; Mohammad, B.; Ismail, M. IoT for healthcare. In *Ultra Low Power ECG Processing System for IoT Devices*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 7–12.
92. Farahani, B.; Firouzi, F.; Chakrabarty, K. Healthcare iot. In *Intelligent Internet of Things: From Device to Fog and Cloud*; Springer: Cham, Switzerland, 2020; pp. 515–545. [\[CrossRef\]](#)
93. Laplante, P.A.; Laplante, N. The internet of things in healthcare: Potential applications and challenges. *IT Prof.* **2016**, *18*, 2–4. [\[CrossRef\]](#)
94. Somasundaram, R.; Thirugnanam, M. Review of security challenges in healthcare internet of things. *Wirel. Netw.* **2021**, *27*, 5503–5509. [\[CrossRef\]](#)
95. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. *Appl. Sci.* **2020**, *2*, 139. [\[CrossRef\]](#)
96. Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet Things J.* **2018**, *5*, 3758–3773. [\[CrossRef\]](#)
97. Mueller, N.; Gerber, J.; Johnston, M. Closing yield gaps through nutrient and water management. *Nature* **2012**, *490*, 254–257. [\[CrossRef\]](#)
98. Tao, W.; Zhao, L.; Wang, G.; Liang, R. Review of the internet of things communication technologies in smart agriculture and challenges. *Comput. Electron. Agric.* **2021**, *189*, 106352. [\[CrossRef\]](#)
99. Verdouw, C.; Wolfert, S.; Tekinerdogan, B. Internet of Things in agriculture. *CABI Rev.* **2016**, *2016*, 1–12. [\[CrossRef\]](#)
100. Tzounis, A.; Katsoulas, N.; Bartzanas, T.; Kittas, C. Internet of Things in agriculture, recent advances and future challenges. *Biosyst. Eng.* **2017**, *164*, 31–48. [\[CrossRef\]](#)
101. Gondchawar, N.; Kawitkar, R.S. IoT based smart agriculture. *Int. J. Adv. Res. Comput. Commun. Eng.* **2016**, *5*, 838–842.
102. Placidi, P.; Gasperini, L.; Grassi, A.; Cecconi, M.; Scorzoni, A. Characterization of low-cost capacitive soil moisture sensors for IoT networks. *Sensors* **2020**, *20*, 3585. [\[CrossRef\]](#)
103. Kour, V.P.; Arora, S. Recent developments of the internet of things in agriculture: A survey. *IEEE Access* **2020**, *8*, 129924–129957. [\[CrossRef\]](#)
104. Dlodlo, N.; Kalezhi, J. The internet of things in agriculture for sustainable rural development. In Proceedings of the 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 13–18.
105. Sinha, B.B.; Dhanalakshmi, R. Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Gener. Comput. Syst.* **2022**, *126*, 169–184. [\[CrossRef\]](#)
106. Rajeswari, S.; Suthendran, K.; Rajakumar, K. A smart agricultural model by integrating IoT, mobile and cloud-based big data analytics. In Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 23–24 June 2017; pp. 1–5.
107. Morais, R.; Mendes, J.; Silva, R.; Silva, N.; Sousa, J.J.; Peres, E. A versatile, low-power and low-cost IoT device for field data gathering in precision agriculture practices. *Agriculture* **2021**, *11*, 619. [\[CrossRef\]](#)
108. Zhang, X.; Cao, Z.; Dong, W. Overview of edge computing in the agricultural internet of things: Key technologies, applications, challenges. *IEEE Access* **2020**, *8*, 141748–141761. [\[CrossRef\]](#)
109. Kassim, M.R.M. IoT applications in smart agriculture: Issues and challenges. In Proceedings of the 2020 IEEE Conference on Open Systems (ICOS), Penang, Malaysia, 17–19 November 2020; pp. 19–24.
110. Burroughs, J. AN236—X-10 Home Automation using the PIC16F877A. Available online: <https://www.yumpu.com/en/document/view/27982893/an236-x-10-home-automation-using-the-pic16f877a-microchip> (accessed on 17 July 2023).
111. Domb, M. Smart home systems based on internet of things. In *Internet of Things (IoT) for Automated and Smart Applications*; IntechOpen: London, UK, 2019.
112. Moser, K.; Harder, J.; Koo, S.G. Internet of things in home automation and energy efficient smart home technologies. In Proceedings of the 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, USA, 5–8 October 2014; pp. 1260–1265.
113. Wang, M.; Zhang, G.; Zhang, C.; Zhang, J.; Li, C. An IoT-based appliance control system for smart homes. In Proceedings of the 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP), Beijing, China, 9–11 June 2013; pp. 744–747.
114. Jo, T.H.; Ma, J.H.; Cha, S.H.N. Elderly perception on the internet of things-based integrated smart-home system. *Sensors* **2021**, *21*, 1284. [\[CrossRef\]](#)
115. Strategy Analytics. Strategy Analytics: Global Smart Home Market Roaring Back in 2021. Business Wire, 6 July 2021. Available online: <https://www.businesswire.com/news/home/20210706005692/en/Strategy-Analytics-Global-Smart-Home-Market-Roaring-Back-in-2021> (accessed on 14 June 2023).
116. Darianian, M.; Michael, M.P. Smart home mobile RFID-based Internet-of-Things systems and services. In Proceedings of the 2008 International Conference on Advanced Computer Theory and Engineering, Phuket, Thailand, 20–22 December 2008; pp. 116–120.

117. Jia, X.; Feng, Q.; Fan, T.; Lei, Q. RFID technology and its applications in Internet of Things (IoT). In Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 21–23 April 2012; pp. 1282–1285.
118. Tan, P.; Wu, H.; Li, P.; Xu, H. Teaching management system with applications of RFID and IoT technology. *Educ. Sci.* **2018**, *8*, 26. [CrossRef]
119. Nisar, K.; Ibrahim, A.A.A.; Park, Y.J.; H Zhou, Y.K.; Memon, S.K.; Naz, N.; Welch, I. Indoor roaming activity detection and analysis of elderly people using RFID technology. In Proceedings of the 2019 1st International Conference on Artificial Intelligence and Data Sciences (AiDAS), Ipoh, Malaysia, 19 September 2019; pp. 174–179.
120. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
121. Samuel, S.S.I. A review of connectivity challenges in IoT-smart home. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–4.
122. Ray, A.K.; Bagwari, A. IoT based Smart home: Security Aspects and security architecture. In Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 10–12 April 2020; pp. 218–222.
123. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, Big Island, HI, USA, 13–17 March 2017; pp. 618–623.
124. Kim, T.H.; Ramos, C.; Mohammed, S. Smart city and IoT. *Future Gener. Comput. Syst.* **2017**, *76*, 159–162. [CrossRef]
125. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
126. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
127. Tragos, E.Z.; Angelakis, V.; Fragkiadakis, A.; Gundlegard, D.; Nechifor, C.S.; Oikonomou, G.; Gavras, A. Enabling reliable and secure IoT-based smart city applications. In Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS), Budapest, Hungary, 24–28 March 2014; pp. 111–116.
128. Khajenasiri, I.; Estebsari, A.; Verhelst, M.; Gielen, G. A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications. *Energy Procedia* **2017**, *111*, 770–779. [CrossRef]
129. Misbahuddin, S.; Zubairi, J.A.; Saggaf, A.; Basuni, J.; Sulaiman, A.; Al-Sofi, A. IoT based dynamic road traffic management for smart cities. In Proceedings of the 2015 12th International Conference on High-Capacity Optical Networks and Enabling/Emerging Technologies (HONET), Islamabad, Pakistan, 21–23 December 2015; pp. 1–5.
130. Sharif, A.; Li, J.; Khalil, M.; Kumar, R.; Sharif, M.I.; Sharif, A. Internet of things—Smart traffic management system for smart cities using big data analytics. In Proceedings of the 2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 15–17 December 2017; pp. 281–284.
131. Rizwan, P.; Suresh, K.; Babu, M.R. Real-time smart traffic management system for smart cities by using Internet of Things and big data. In Proceedings of the 2016 International Conference on Emerging Technological Trends (ICETT), Kollam, India, 21–22 October 2016; pp. 1–7.
132. Javaid, S.; Sufian, A.; Pervaiz, S.; Tanveer, M. Smart traffic management system using Internet of Things. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 11–14 February 2018; pp. 393–398.
133. Rabby, M.K.M.; Islam, M.M.; Imon, S.M. A review of IoT application in a smart traffic management system. In Proceedings of the 2019 5th International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, Bangladesh, 26–28 September 2019; pp. 280–285.
134. Kaza, S.; Yao, L.C.; Bhada-Tata, P.; Van Woerden, F. *What a Waste 2.0: A Global Snapshot of Solid Waste Management to 2050*; Urban Development; World Bank: Washington, DC, USA, 2018. Available online: <https://openknowledge.worldbank.org/handle/10986/30317> (accessed on 24 April 2020).
135. Haribabu, P.; Kassa, S.R.; Nagaraju, J.; Karthik, R.; Shirisha, N.; Anila, M. Implementation of an smart waste management system using IoT. In Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 7–8 December 2017; pp. 1155–1156.
136. Oralhan, Z.; Oralhan, B.; Yigit, Y. Smart city application: Internet of things (IoT) technologies based smart waste collection using data mining approach and ant colony optimization. *Int. Arab. J. Inf. Technol.* **2017**, *14*, 423–427.
137. Mdukaza, S.; Isong, B.; Dladlu, N.; Abu-Mahfouz, A.M. Analysis of IoT-enabled solutions in smart waste management. In Proceedings of the IECON 2018–44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 4639–4644.
138. Hasan, B.M.; Yeazdani, A.M.M.; Istiaque, L.M.; Chowdhury, R.M.K. Smart Waste Management System Using IoT. Ph.D. Thesis, BRAC University, Dhaka, Bangladesh, 2017.
139. Chen, E.T. The internet of things: Opportunities, issues, and challenges. In *The Internet of Things in the Modern Business Environment*; IGI Global: Hershey, PA, USA, 2017; pp. 167–187.

140. Gutierrez, J.M.; Jensen, M.; Henius, M.; Riaz, T. Smart waste collection system based on location intelligence. *Procedia Comput. Sci.* **2015**, *61*, 120–127. [\[CrossRef\]](#)
141. Dais, S. Industry 4.0—Offense, vision, approach. In *Industry 4.0 in Production, Automation and Logistics. Application, Technologies and Migration*; Springer: Wiesbaden, Switzerland, 2014; pp. 625–634.
142. Kolberg, D.; Zuhlke, D. Lean automation enabled by Industry 4.0 technologies. *IFAC PapersOnLine* **2015**, *48*, 1870–1875. [\[CrossRef\]](#)
143. Bartodziej, C.J. *The Concept Industry 4.0—An Empirical Analysis of Technologies and Applications in Production Logistics*; Springer Fachmedien Wiesbaden: Wiesbaden, Switzerland, 2017.
144. Shrouf, F.; Ordieres, J.; Miragliotta, G. Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Selangor, Malaysia, 9–12 December 2014; pp. 697–701.
145. Yin, Y.; Stecke, K.E.; Li, D. The evolution of production systems from Industry 2.0 through Industry 4.0. *Int. J. Prod. Res.* **2018**, *56*, 848–861. [\[CrossRef\]](#)
146. Sarker, I.H.; Khan, A.I.; Abushark, Y.B.; Alsolami, F. Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions. In *Mobile Networks and Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 1–17.
147. Seralathan, Y.; Oh, T.T.; Jadhav, S.; Myers, J.; Jeong, J.P.; Kim, Y.H.; Kim, J.N. IoT security vulnerability: A case study of a Web camera. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 11–14 February 2018; pp. 172–177.
148. De Donno, M.; Dragoni, N.; Giaretta, A.; Spognardi, A. DDoS-capable IoT malwares: Comparative analysis and Mirai investigation. *Secur. Commun. Netw.* **2018**, *2018*, 7178164. [\[CrossRef\]](#)
149. Kambourakis, G.; Kolias, C.; Stavrou, A. The mirai botnet and the iot zombie armies. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 267–272.
150. Su, J.; Vasconcellos, D.V.; Prasad, S.; Sgurra, D.; Feng, Y.; Sakurai, K. Lightweight classification of IoT malware based on image recognition. In Proceedings of the 2018 IEEE 42Nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; Volume 2, pp. 664–669.
151. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [\[CrossRef\]](#)
152. Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O.B. Internet of Things (IoT): Taxonomy of security attacks. In Proceedings of the 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11–12 August 2016; pp. 321–326.
153. Bertino, E.; Islam, N. Botnets and internet of things security. *Computer* **2017**, *50*, 76–79. [\[CrossRef\]](#)
154. You, I.; Trnka, M.; Cerny, T.; Stickney, N. Survey of Authentication and Authorization for the Internet of Things. *Secur. Commun. Netw.* **2018**, *2018*, 4351603. [\[CrossRef\]](#)
155. Santoso, F.K.; Vun, N.C. Securing IoT for smart home system. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015; pp. 1–2.
156. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in internet of things: Taxonomies and open challenges. *Mob. Netw. Appl.* **2019**, *24*, 796–809. [\[CrossRef\]](#)
157. Lee, E.; Seo, Y.D.; Oh, S.R.; Kim, Y.G. A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1020–1047. [\[CrossRef\]](#)
158. Salman, T.; Jain, R. Networking protocols and standards for internet of things. In *Internet of Things and Data Analytics Handbook*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 215–238.
159. Pal, A.; Rath, H.K.; Shailendra, S.; Bhattacharyya, A. IoT standardization: The road ahead. In *Internet of Things-Technology, Applications and Standardization*; IntechOpen: London, UK, 2018; pp. 53–74.
160. Bröring, A.; Ziller, A.; Charpenay, V.; Thuluva, A.S.; Anicic, D.; Schmid, S.; Seidel, C. The big iot api-semantically enabling iot interoperability. *IEEE Pervasive Comput.* **2018**, *17*, 41–51. [\[CrossRef\]](#)
161. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700. [\[CrossRef\]](#)
162. Stergiou, C.; Psannis, K.E.; Gupta, B.B.; Ishibashi, Y. Security, privacy efficiency of sustainable cloud computing for big data IoT. *Sustain. Comput. Inform. Syst.* **2018**, *19*, 174–184. [\[CrossRef\]](#)
163. Sadeeq, M.M.; Abdulkareem, N.M.; Zeebaree, S.R.; Ahmed, D.M.; Sami, A.S.; Zebari, R.R. IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Acad. J.* **2021**, *1*, 1–7. [\[CrossRef\]](#)
164. Lu, Y.; Da Xu, L. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Things J.* **2018**, *6*, 2103–2115. [\[CrossRef\]](#)
165. Biswas, A.R.; Giaffreda, R. IoT and cloud convergence: Opportunities and challenges. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Republic of Korea, 6–8 March 2014; pp. 375–376.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.