Review

Not peer-reviewed version

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

Robin Chataut * and Alex Phoummalayvane

Posted Date: 1 June 2023

doi: 10.20944/preprints202306.0002.v1

Keywords: IoT; Smart Cities; Internet-of-Medical-Things; Sensors; Security

Review

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

Alex Phoummalayvane † and Robin Chataut *,†

Computer Science Department, Fitchburg State University, Fitchburg, MA 01420, USA
* Correspondence: rchataut@fitchburgstate.edu
† These authors contributed equally to this work.

Abstract: The Internet of Things (IoT) technology and devices constitute an exciting field in computer science that is rapidly emerging worldwide. IoT devices function by connecting real-world objects to the internet, resulting in a higher number of interconnected devices than ever witnessed in history. Through internet connectivity, these devices can be utilized in various ways, such as monitoring and tracking. Their prevalence is increasing exponentially, coinciding with advancements in wireless networking technologies. The internet's enhanced connectivity has played a vital role in fostering the proliferation of IoT devices. Presently, almost any everyday object can be network-connected. The demand for automation and efficiency has also been a contributing factor to the advancements in this technology. This paper aims to review the emergence of IoT devices, analyze their common applications, and explore 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. IoT technology can be applied to nearly any domain, and each use case has unique requirements. 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. Moreover, a comprehensive understanding of the prevalent methodologies will enable readers to distinguish between current practices and future methods. Given the rapid rate at which IoT technology is advancing, this paper aims to provide researchers with an understanding of the factors that have brought us to this point and the ongoing efforts to shape the future of IoT.

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

1. Introduction

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 that exist, so the amount of connectivity that IoT devices hold is enormous [2]. In order to better understand where the future of IoT technology is, it is important to understand the unique circumstances that brought IoT to this point. A key distinction to make between the internet and IoT is that the internet is a mesh of networks, whereas IoT is an internet of devices [3,4]. An early example of the first IoT device was John Romkey's first turning a toaster 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 an interconnection of sending and actuating devices that provide the ability to share information across different platforms [7–18].

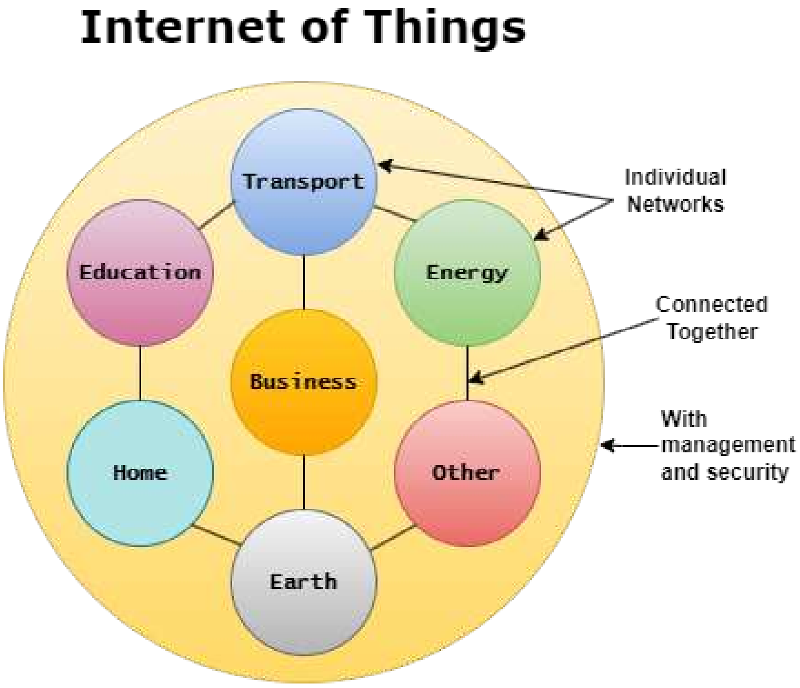


Figure 1. Broad overview of IoT technology.

The rapid rise of technology and the capabilities of computer systems 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, moving towards the future. This paper analyzes different applications of IoT technology in fields like healthcare and agriculture. Ultimately, the number of IoT applications seems endless and growing as the years go on.

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.

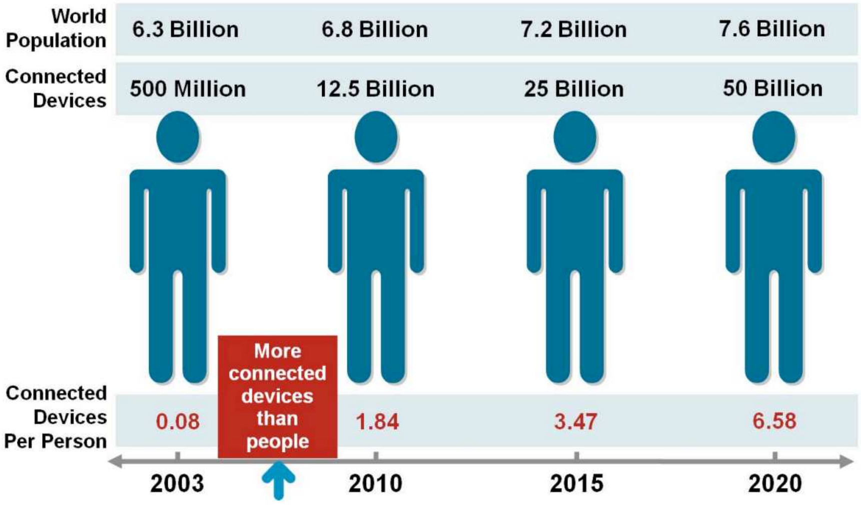


Figure 2. Number of IoT Devices is Greater than Number of People.

Many different strategies are being utilized by computing professionals in order to advance the field of research in regards to IoT technology [19–23]. In particular, machine learning and artificial intelligence have played a key role in advancing this emerging field of computer science and will continue to do so in new and exciting ways [19–24]. 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 done to advance IoT technologies.

2. Applications of IoT Devices

Since internet-of-things can be understood by seeing them as devices/objects that are connected to a network, the applications of IoT devices are endless [24–31]. Leaders of different companies/organizations are realizing the potential that IoT has to make an impact and are investing more in these key pieces of technology in order to reap the benefits [32]. Nearly any object can be outfitted with the appropriate technology that will be involved in the data transmission coming from IoT devices and their connected networks. Writing about all the different applications would be a long and arduous process and it can be more beneficial in the beginning to first understand the most common applications of IoT devices before exploring what the future holds.

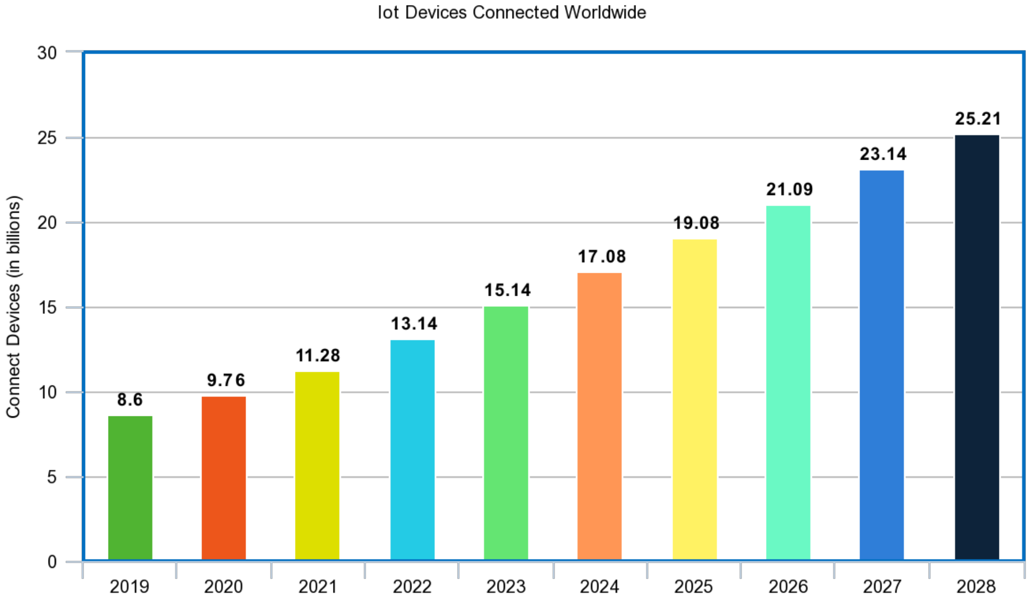
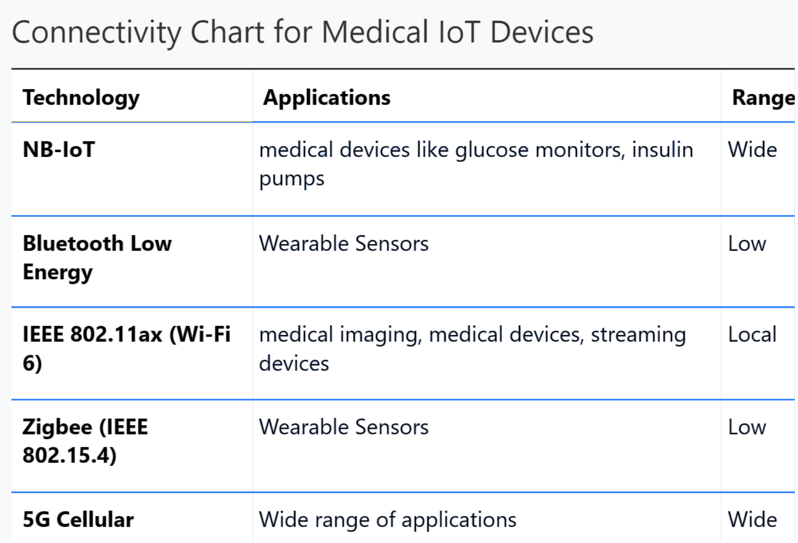


Figure 3. Number of IoT Devices Globally.

2.2. 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 like the AliveCor heart monitor, which relies on IoT sensors, show how useful technology can be when applied to healthcare in efforts to save lives [33]. Advances in technology have always played a major role in healthcare and there are many different applications in which IoT devices are used 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 hospitals [34]. The information that is collected from IoT devices is helpful in the medical setting because it can be analyzed and used in ways such as early disease prediction [35]. IoT sensors even played a critical role during the COVID-19 pandemic in helping health workers better monitor critical parameters that could save lives if changes were detected right away [36]. By examining all of these different applications of IoT devices in the healthcare industry, researchers can find additional rooms to advance this field.



Connectivity Chart for Medical IoT Devices

Technology	Applications	Range
NB-IoT	medical devices like glucose monitors, insulin pumps	Wide
Bluetooth Low Energy	Wearable Sensors	Low
IEEE 802.11ax (Wi-Fi 6)	medical imaging, medical devices, streaming devices	Local
Zigbee (IEEE 802.15.4)	Wearable Sensors	Low
5G Cellular	Wide range of applications	Wide

Figure 4. Connectivity of Different Medical IoT Devices.

The use of sensors in healthcare is one way that IoT devices play a critical role in the delivery of healthcare services [37]. These sensors are basically acting as a bridge between the physical and information world by collecting a variety of types of data [5]. 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 [38]. These 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 [39]. 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 [40]. 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 deep role in creating stronger healthcare systems and the future of healthcare will become increasingly reliant on technology [41].

Medical sensors are important in collecting useful information about a patient's health but 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 but it matters even more in a situation like healthcare where IoT devices will be collecting sensitive information about patients that is private in nature [42]. If a patient's medical information were to get compromised, this could lead to consequences to those hospital organizations that did not employ the proper security measures to prevent it. The privacy and confidentiality of a patient's medical information is a core concern when addressing the security vulnerabilities of healthcare IoT devices [43].

There are many issues that present a challenge to the successful use of IoT devices in healthcare and it is important to address these issues thoroughly when handling mission-critical operations like that of healthcare. Some important limitations that influence the use of IoT technology in medical devices include the need for high power consumption, availability of limited resources, and handling security issues from the large number of devices being used [44].

The use of IoT technology in healthcare is promising and exciting. There are many useful applications in which 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.

2.3. 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 advancements in smart agriculture [45]. On top of the growing demand, things such as climate change and water scarcity have also played a role in increasing the demand for more efficient agriculture systems [46]. Much of the technology around IoT implementation aims to reduce resource wasting in agriculture [47]. The use of IoT technology in agricultural settings is critical in maintaining efficient operations and represents another common use-case of IoT technology. The demand for food supply chains that are of quality and quantity is important in feeding the world and having efficient systems built around these supply chains will benefit people all over the world [48]. The need for more efficient food-delivery systems is what helped promote IoT use in agriculture because stakeholders saw the benefits that technology could provide [49].

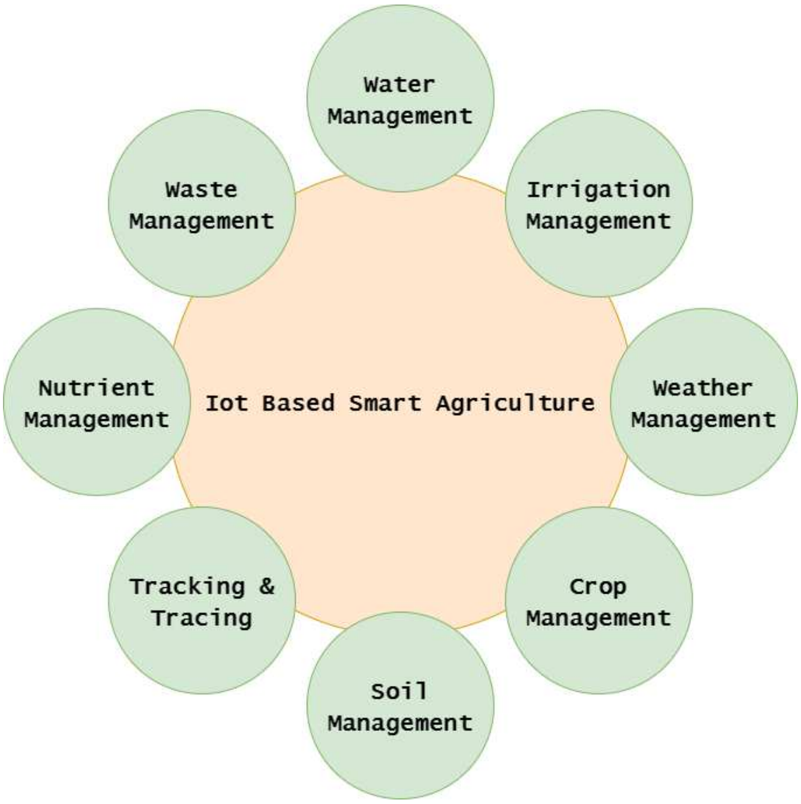


Figure 5. Different Types of Agriculture Applications for IoT.

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 a key proponent in helping IoT devices achieve their automation goals [50]. This can be useful in massive operations like 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 [51]. These IoT devices can be used to measure soil conditions such as water content and give an appropriate signal 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 [52].

Data analytics is another area in which IoT has an important role in agriculture. Collecting and analyzing data is very useful because it can give important insights into how effective or ineffective an operation is. This data can be used to give stakeholders important insight that will ultimately impact their decision-making [53]. IoT devices collect massive amounts of data and this data is useful when analyzed over time to help aid in decisions about estimation and forecasting [54]. In particular, IoT devices can be used to gather massive amounts of information that will help those involved in agriculture maximize their yields. IoT devices contribute to the gathering of massive amounts of data that can be analyzed using machine learning methods that impact prediction, storage management, decision-making, farm management, and precision farming [45]. This data can become useful when trying to implement more sustainable farming methods through the use of data-driven decision-making [53].

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 [55]. 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 [56]. 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 [57]. In addition to this, many farmers in rural parts of the world have limited knowledge of how to use IoT devices [58].

2.4. Smart-Home Applications

Smart home applications represent a promising use case in which people benefit from IoT technology and there are numerous advantages/disadvantages to consider. These smart home devices date back to the 1970s when the X10 protocol was first conceived and this technology allowed for smart home devices to communicate properly [59]. 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 [60]. Home automation remains a core feature around which IoT technology is applied to [61]. 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 [62]. There are many benefits that extend beyond convenience. The use 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 [63].

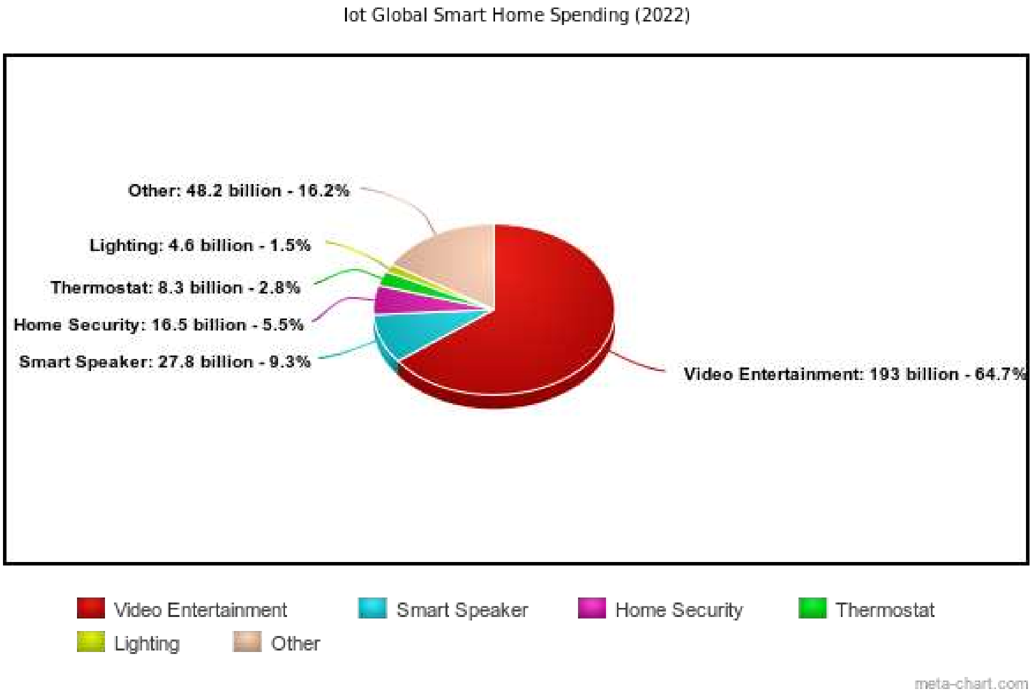


Figure 6. Smart Home Spending Statistics.

There are many techniques utilized in order to bring smart home technology to life. One important method relies on Radio Frequency Identification (RFID) systems being used in order to act as an enabler technology for IoT [64]. RFID is an important technology that helps in identifying objects, recording data, and even controlling individual targets through the use of radio waves [65]. RFID devices can be used in a variety of ways. For example, higher education institutions can utilize RFID technology in student identification cards [66]. RFID technology is also used to detect indoor roaming activity of the elderly and the data collected is used to give more insight into the health of elderly who live alone [67].

In an ideal future, IoT devices should be able to communicate with each other seamlessly [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 integration of devices is one concern moving forward [69]. Different technologies utilized by IoT devices in order to create this connectivity include things such as WiFi, ZigBee, Z-Wave, Bluetooth LE, and Thread [68].

Security and privacy are also important to consider because smart grid technology can be a target for cyber attacks [69]. There are so many IoT objects that can be used in homes and this dynamic and heterogeneous nature of smart home environments presents a challenge when it comes to addressing authentication and privacy issues [19]. Cyber attackers could target items such as smart home routers, gateways, or any other IoT-enabled devices to access data [71]. 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 [22]). Although blockchain approaches have benefited from decentralized security/privacy, there are drawbacks when it comes to the energy and computational overhead that makes it not ideal for IoT devices that are resource restrained [72].

2.5. 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 and is used to make important decisions in city operations [73]. These systems are inherently complex due to a large number of devices, link layer technologies, and the different services involved in the operation of smart city technology [74]. 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 [75]. The use of IoT technology to enable smart cities is useful due to the quality of life it improves to the citizens within those cities [76]. The goal of smart cities is to use all this information that is collected from IoT devices in order to improve the performance of urban services to citizens and also consider resource consumption at the same time [77].

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 [78]. A Smart Traffic System (STS) involves real-time data collection and requires IoT devices to quickly obtain real-time public traffic data and get it processed [79]. The sensors used in smart traffic management systems can be embedded into roads in order to detect vehicles every 500 or 1000 meters [80]. Cameras are able to apply digital image processing techniques and consequently apply algorithms to aid in the prediction of traffic density, and this information is then used accordingly [81]. Aside from just helping traffic flow, smart traffic management systems also help with improving air quality and providing safety for the elderly [82].

Some research indicates that the amount of solid waste will one day reach around 3.4 billion tons by the year 2050, and that would put a tremendous strain on municipal waste management systems [19,83]. 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 that highly-populated urban areas present [84]. 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 [85]. Some major factors that are driving the need for smart waste management include the need for more energy-efficient processes and healthier environments within cities [86]. A number of different objects can be repurposed into IoT devices, such as trash and recycling containers [87] and different technologies can be used to indicate when it is time to service a full container. In addition to sending when waste bins are full, some sensors are even able to detect unpleasant smells through the use of gas sensors [88]. 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 [89].

2.6. 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 [90–94]. 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.

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 a crucial role 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. Designed to be safe, adaptable, and easily programmable, cobots 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.

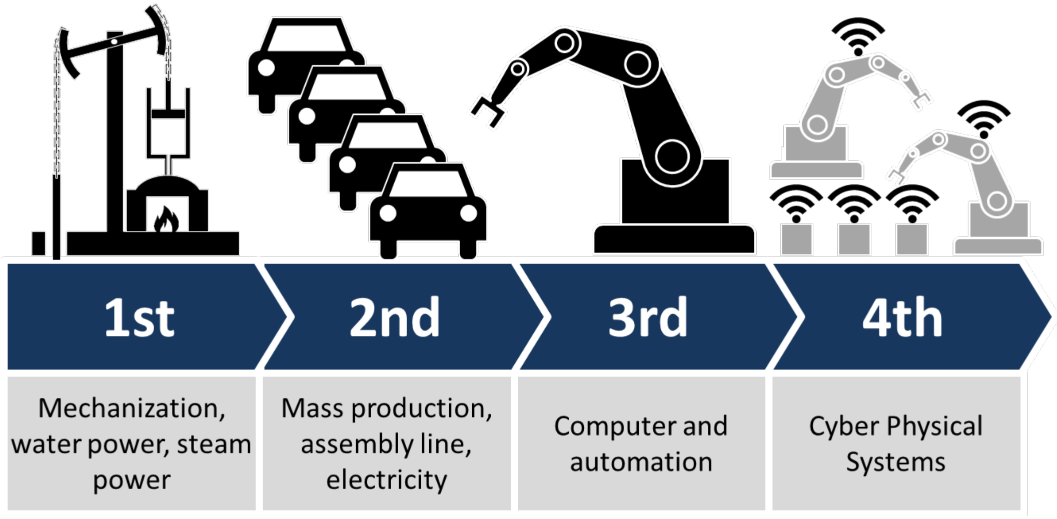

1st
2nd
3rd
4th
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems

Figure 7. Industry 4.0.

3. Challenges and Active Research Topics

3.1. Security of IoT Devices

The use of internet-of-things devices is becoming an increasingly larger part of the daily lives of people around the world; however, cyberattacks remain a large threat to the safe use of IoT [95]. 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 do harm or use this data for nefarious purposes. In one case, there were even attacks that could target IoT devices like the Mirai malware [96], which would hack/convert devices into its botnet and carry out DDoS attacks [97]. Malware like the Mirai and others take advantage of the vast amount of poorly protected IoT devices which commonly suffer from poor configurations and open design, and make them targets [98]. 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 [99]. 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 [100].

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 [101]. Hackers and criminals could seriously impact the expansion of IoT devices into the future, and it is crucial that security is thoroughly researched to mitigate these negative impacts.

doi:10.20944/preprints202306.0002.v1

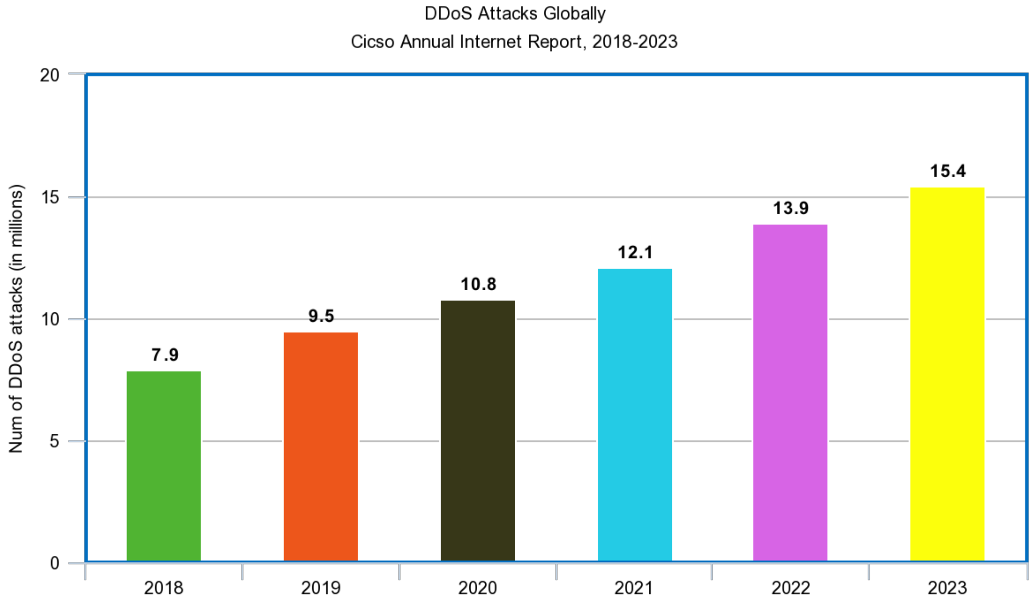


Figure 8. DDoS attacks Worldwide.

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 trying to gain access to them. These passwords can often be weak, and criminals can have easy access to the IoT device. There is a lack of standardization revolving around how complex passwords should be. There is research out there that shows evidence of how having more complex password combinations in IoT devices can prevent more cyber attacks [102]. 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 [103]. Authentication is the process of how we verify users are who they say they are 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 which 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 [104].

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 the 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 by use of the one-time password, and it verifies that the password was sourced from a valid location [23].

3.3. Interoperability Challenges

Being able to use IoT devices and make them work smoothly and without compatibility issues remains a challenge 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 [105]. The need for safe interoperability of IoT devices has even led to the creation of international organizations which develop standards that IoT devices can adopt with the intention of becoming more compatible [106]. The use of protocols and standards, such as Bluetooth and ZigBee, is critical to the rise of IoT because it essentially establishes the rules for use and communication, which helps address interoperability concerns [107]. International organizations like IEEE, Internet Engineering Task Force (IETF), OneM2M, and others have developed important standards and protocols and play an integral role in influencing the IoT [108]. An important contribution to addressing these challenges was the creation of the BiG IoT project, which was an initiative that sought to create a common API through which different IoT devices could communicate through [70].

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. CloudIoT is a novel IT paradigm that represents the merging of cloud with IoT, and research in this area will be crucial in moving this technology forward [109]. Cloud computing is essentially an extension of distributed computing, parallel computing, and grid computing [75]. There are many IoT constraints that cloud computing addresses, such as processing, storage, and communication [110]. For example, a major concern about IoT data is in regards to the security risks that come from storing data locally on IoT devices [111], and cloud computing aims to address this concern by allowing data storage in cloud computing servers [112]. Since data collected from IoT devices is often unstructured, cloud computing research looks to improve the real-time data processing capabilities and allow for more dynamic resource management [113].

4. Conclusion

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, that 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 a vital role 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 sum up, IoT technology has brought about a revolution across 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: The authors declare that they have equally contributed to the paper. All authors read and approved the final manuscript.

Funding: This research received no external funding.

Acknowledgments: We want to thank the authors of the literature cited in this paper for contributing 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

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. (2020). Building smart cities applications based on IoT technologies: A review. Technology Reports of Kansai University, 62(3), 1083-1092.
2. Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. International Journal of Computer Networks, 5(1), 1-17.
3. Paul, C., Ganesh, A., & Sunitha, C. (2018, January). An overview of IoT based smart homes. In 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp. 43-46). IEEE.
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. (2014, November). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In 2014 International conference on science engineering and management research (ICSEMR) (pp. 1-8). IEEE.
6. Al-Khafajiy, M., Webster, L., Baker, T., & Waraich, A. (2018, June). 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 (pp. 1-7).
7. Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. Journal of Network and Computer Applications, 97, 48-65.
8. Sharma, S.; Kaushik, B. A survey on Internet of vehicles: Applications, security issues and solutions. *Veh. Commun.* 2019, 20, 100182. **[Google Scholar] [CrossRef]**
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. **[Google Scholar] [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. **[Google Scholar] [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. (2017). Implementation of IoT architecture for SMART HOME using GSM technology. *International Journal of Computer Techniques*, 4(1), 42-48.
13. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). 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*, 8, 23022-23040.
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. *Universal Access in the Information Society*, 18(4), 837–869, 2019.

15. Ahad, A., Tahir, M., & Yau, K. A. 5g-based smart healthcare network: Architecture, taxonomy, challenges and future research directions. *IEEE Access*, 7, 100747–100762, 2019.
16. Ramachandran, A., Pahwa, P., & K.R., A. Machine learning-based techniques for fall detection in geriatric healthcare systems. In 2018 9th International Conference on Information Technology in Medicine and Education (ITME), pages 232–237, 2018.
17. Shaikh, Y., Parvati, V. K., & Biradar, S. R. Survey of smart healthcare systems using internet of things (IoT): (invited paper). In 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), pages 508–513, 2018.
18. Rajini, N. H. A comprehensive survey on internet of things based healthcare services and its applications. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pages 483–488, 2019.
19. Ali, T., Irfan, M., Alwadie, A. S., & Glowacz, A. (2020). IoT-based smart waste bin monitoring and municipal solid waste management system for smart cities. Arabian Journal for Science and Engineering, 45, 10185-10198.
20. Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017, September). IoT based smart home: Security challenges, security requirements and solutions. In 2017 23rd International Conference on Automation and Computing (ICAC) (pp. 1-6). IEEE.
21. Alotaibi, M. (2021). Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN. IEEE Access, 9, 159187-159197. https://doi.org/10.1109/ACCESS.2021.3130005
22. Arif, S., Khan, M. A., Rehman, S. U., Kabir, M. A., & Imran, M. (2020). Investigating smart home security: Is blockchain the answer?. IEEE Access, 8, 117802-117816.
23. Atwady, Y., & Hammoudeh, M. (2017, July). A survey on authentication techniques for the internet of things. In Proceedings of the International Conference on Future Networks and Distributed Systems.
24. Morgan, J. (2014). A simple explanation of the internet of things'. Retrieved November, 20, 2015.
25. Chen, W. E., Wang, Y. H., Huang, P. C., Huang, Y. Y., & Tsai, M. Y. (2018, August). A smart IoT system for waste management. In 2018 1st International cognitive cities conference (IC3) (pp. 202-203). IEEE.
26. Durga, S., Nag, R., & Daniel, E. (2019, March). Survey on machine learning and deep learning algorithms used in internet of things (IoT) healthcare. In 2019 3rd international conference on computing methodologies and communication (ICCMC) (pp. 1018-1022). IEEE.
27. Hsu, H.-T., Jong, G.-J., Chen, J.-H., & Jhe, C.-G. (2019). Improve Iot Security System Of Smart-Home By Using Support Vector Machine. In 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS). 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS). IEEE. https://doi.org/10.1109/ccoms.2019.8821678
28. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686-1721.
29. Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. J. Commun., 12(4), 240-247.
30. Ojha, T., Misra, S., & Raghuwanshi, N. S. (2015). Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. Computers and electronics in agriculture, 118, 66-84.
31. Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010, January). Cloud computing research and development trend. In 2010 Second international conference on future networks (pp. 93-97). IEEE.
32. Pardini, K., Rodrigues, J. J., Diallo, O., Das, A. K., de Albuquerque, V. H. C., & Kozlov, S. A. (2020). A smart waste management solution geared towards citizens. Sensors, 20(8), 2380.
33. Halcox, J. P., Wareham, K., Cardew, A., Gilmore, M., Barry, J. P., Phillips, C., & Gravenor, M. B. (2017). Assessment of remote heart rhythm sampling using the AliveCor heart monitor to screen for atrial fibrillation: the REHEARSE-AF study. Circulation, 136(19), 1784-1794.
34. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. Ieee Access, 5, 26521-26544.
35. Khan, M. A. (2021). Challenges facing the application of IoT in medicine and healthcare. International Journal of Computations, Information and Manufacturing (IJCIM), 1(1).
36. Javaid, M., & Khan, I. H. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. Journal of Oral Biology and Craniofacial Research, 11(2), 209-214.

37. Shah, S. T. U., Yar, H., Khan, I., Ikram, M., & Khan, H. (2019). Internet of things-based healthcare: recent advances and challenges. Applications of Intelligent Technologies in Healthcare, 153-162.
38. Yuehong, Y. I. N., Zeng, Y., Chen, X., & Fan, Y. (2016). The internet of things in healthcare: An overview. Journal of Industrial Information Integration, 1, 3-13.
39. Maksimović, M., Vujović, V., & Perišić, B. (2015, June). A custom Internet of Things healthcare system. In 2015 10th iberian conference on information systems and technologies (CISTI) (pp. 1-6). IEEE.
40. Tekeste Habte, T., Saleh, H., Mohammad, B., Ismail, M., Tekeste Habte, T., Saleh, H., ... & Ismail, M. (2019). IoT for healthcare. Ultra Low Power ECG Processing System for IoT Devices, 7-12.
41. Farahani, B., Firouzi, F., & Chakrabarty, K. (2020). Healthcare iot. Intelligent Internet of Things: From Device to Fog and Cloud, 515-545.
42. Laplante, P. A., & Laplante, N. (2016). The internet of things in healthcare: Potential applications and challenges. It Professional, 18(3), 2-4.
43. Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare internet of things. Wireless Networks, 27, 5503-5509.
44. Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: a systematic review. SN Applied Sciences, 2(1), 139.
45. Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet of things Journal, 5(5), 3758-3773.
46. Mueller, N., Gerber, J., Johnston, M. et al. Closing yield gaps through nutrient and water management. Nature 490, 254–257 (2012). https://doi.org/10.1038/nature11420
47. Tao, W., Zhao, L., Wang, G., & Liang, R. (2021). Review of the internet of things communication technologies in smart agriculture and challenges. Computers and Electronics in Agriculture, 189, 106352.
48. Verdouw, C., Wolfert, S., & Tekinerdogan, B. (2016). Internet of Things in agriculture. CABI Reviews, (2016), 1-12.
49. Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of Things in agriculture, recent advances and future challenges. Biosystems engineering, 164, 31-48.
50. Gondchawar, N., & Kawitkar, R. S. (2016). IoT based smart agriculture. International Journal of advanced research in Computer and Communication Engineering, 5(6), 838-842.
51. Placidi, P., Gasperini, L., Grassi, A., Cecconi, M., & Scorzoni, A. (2020). Characterization of low-cost capacitive soil moisture sensors for IoT networks. Sensors, 20(12), 3585.
52. Kour, V. P., & Arora, S. (2020). Recent developments of the internet of things in agriculture: a survey. Ieee Access, 8, 129924-129957.
53. Dlodlo, N., & Kalezhi, J. (2015, May). The internet of things in agriculture for sustainable rural development. In 2015 international conference on emerging trends in networks and computer communications (ETNCC) (pp. 13-18). IEEE.
54. Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. Future Generation Computer Systems, 126, 169-184.
55. Rajeswari, S. K. R. K. A., Suthendran, K., & Rajakumar, K. (2017, June). A smart agricultural model by integrating IoT, mobile and cloud-based big data analytics. In 2017 international conference on intelligent computing and control (I2C2) (pp. 1-5). IEEE.
56. Morais, R., Mendes, J., Silva, R., Silva, N., Sousa, J. J., & Peres, E. (2021). A versatile, low-power and low-cost IoT device for field data gathering in precision agriculture practices. Agriculture, 11(7), 619.
57. Zhang, X., Cao, Z., & Dong, W. (2020). Overview of edge computing in the agricultural internet of things: key technologies, applications, challenges. Ieee Access, 8, 141748-141761.
58. Kassim, M. R. M. (2020, November). Iot applications in smart agriculture: Issues and challenges. In 2020 IEEE conference on open systems (ICOS) (pp. 19-24). IEEE.
59. Burroughs, J. (2010). X-10® home automation using the PIC16F877A. Lamp, 10(10).
60. Domb, M. (2019). Smart home systems based on internet of things. In Internet of Things (IoT) for automated and smart applications. IntechOpen.
61. Moser, K., Harder, J., & Koo, S. G. (2014, October). Internet of things in home automation and energy efficient smart home technologies. In 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 1260-1265). IEEE.

62. Wang, M., Zhang, G., Zhang, C., Zhang, J., & Li, C. (2013, June). An IoT-based appliance control system for smart homes. In 2013 fourth international conference on intelligent control and information processing (ICICIP) (pp. 744-747). IEEE.
63. Jo, T. H., Ma, J. H., & Cha, S. H. (2021). Elderly perception on the internet of things-based integrated smart-home system. Sensors, 21(4), 1284.
64. Darianian, M., & Michael, M. P. (2008, December). Smart home mobile RFID-based Internet-of-Things systems and services. In 2008 International conference on advanced computer theory and engineering (pp. 116-120). IEEE.
65. Jia, X., Feng, Q., Fan, T., & 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.
66. Tan, P., Wu, H., Li, P., & Xu, H. (2018). Teaching management system with applications of RFID and IoT technology. Education Sciences, 8(1), 26.
67. Nisar, K., Ibrahim, A. A. A., Park, Y. J., Hzou, Y. K., Memon, S. K., Naz, N., & Welch, I. (2019, September). Indoor roaming activity detection and analysis of elderly people using RFID technology. In 2019 1st international conference on artificial intelligence and data sciences (AiDAS) (pp. 174-179). IEEE.
68. Samuel, S. S. I. (2016, March). A review of connectivity challenges in IoT-smart home. In 2016 3rd MEC International conference on big data and smart city (ICBDSC) (pp. 1-4). IEEE.
69. Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of cleaner production, 140, 1454-1464.
70. Bröring, A., Ziller, A., Charpenay, V., Thuluva, A. S., Anicic, D., Schmid, S., ... & Seidel, C. (2018). The big iot api-semantically enabling iot interoperability. IEEE Pervasive Computing, 17(4), 41-51.
71. Ray, A. K., & Bagwari, A. (2020, April). IoT based Smart home: Security Aspects and security architecture. In 2020 IEEE 9th international conference on communication systems and network technologies (CSNT) (pp. 218-222). IEEE.
72. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.
73. Kim, T. H., Ramos, C., & Mohammed, S. (2017). Smart city and IoT. Future Generation Computer Systems, 76, 159-162.
74. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), 22-32.
75. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122-129. Sent message.
76. Tragos, E. Z., Angelakis, V., Fragkiadakis, A., Gundlegard, D., Nechifor, C. S., Oikonomou, G., ... & Gavras, A. (2014, March). Enabling reliable and secure IoT-based smart city applications. In 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS) (pp. 111-116). IEEE.
77. Khajenasiri, I., Estebsari, A., Verhelst, M., & Gielen, G. (2017). A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications. Energy Procedia, 111, 770-779.
78. Misbahuddin, S., Zubairi, J. A., Saggaf, A., Basuni, J., Sulaiman, A., & Al-Sofi, A. (2015, December). IoT based dynamic road traffic management for smart cities. In 2015 12th International conference on high-capacity optical networks and enabling/emerging technologies (HONET) (pp. 1-5). IEEE.
79. Sharif, A., Li, J., Khalil, M., Kumar, R., Sharif, M. I., & Sharif, A. (2017, December). Internet of things—smart traffic management system for smart cities using big data analytics. In 2017 14th international computer conference on wavelet active media technology and information processing (ICCWAMTIP) (pp. 281-284). IEEE.
80. Rizwan, P., Suresh, K., & Babu, M. R. (2016, October). Real-time smart traffic management system for smart cities by using Internet of Things and big data. In 2016 international conference on emerging technological trends (ICETT) (pp. 1-7). IEEE.
81. Javaid, S., Sufian, A., Pervaiz, S., & Tanveer, M. (2018, February). Smart traffic management system using Internet of Things. In 2018 20th international conference on advanced communication technology (ICACT) (pp. 393-398). IEEE.

doi:10.20944/preprints202306.0002.v1

82. Rabby, M. K. M., Islam, M. M., & Imon, S. M. (2019, September). A review of IoT application in a smart traffic management system. In 2019 5th International Conference on Advances in Electrical Engineering (ICAEE) (pp. 280-285). IEEE.
83. 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; Washington, DC: World Bank. © World Bank. https://openknowledge.worldbank.org/handle/10986/30317. Accessed 24 Apr 2020
84. Haribabu, P., Kassa, S. R., Nagaraju, J., Karthik, R., Shirisha, N., & Anila, M. (2017, December). Implementation of an smart waste management system using IoT. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 1155-1156). IEEE
85. Oralhan, Z., Oralhan, B., & Yiğit, Y. (2017). Smart city application: Internet of things (IoT) technologies based smart waste collection using data mining approach and ant colony optimization. Internet Things, 14(4), 5.
86. Mdukaza, S., Isong, B., Dladlu, N., & Abu-Mahfouz, A. M. (2018, October). Analysis of IoT-enabled solutions in smart waste management. In IECON 2018-44th annual conference of the IEEE industrial electronics society (pp. 4639-4644). IEEE.
87. Hasan, B. M., Yeazdani, A. M. M., Istiaque, L. M., & Chowdhury, R. M. K. (2017). Smart waste management system using IoT (Doctoral dissertation, BRAC University).
88. Chen, E. T. (2017). The internet of things: Opportunities, issues, and challenges. In The internet of things in the modern business environment (pp. 167-187). IGI global.
89. Gutierrez, J. M., Jensen, M., Henius, M., & Riaz, T. (2015). Smart waste collection system based on location intelligence. Procedia Computer Science, 61, 120-127.
90. S. Dais, "Industry 4.0—offense, vision, approach," in Industry 4.0 in production, automation and logistics. Application, technologies and migration, Springer, Wiesbaden, 2014, pp. 625-634.
91. D. Kolberg and D. Zuhlke, "Lean automation enabled by Industry 4.0 technologies," IFAC PapersOnLine, vol. 48, no. 3, pp. 1870-1875, 2015.
92. C. J. Bartodziej, "The concept Industry 4.0—an empirical analysis of technologies and applications in production logistics," Springer Fachmedien Wiesbaden, Wiesbaden, 2017.
93. F. Shrouf, J. Ordieres, and G. Miragliotta, "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 publisher: IEEE," in 2014 IEEE international conference on industrial engineering and engineering management, 2014, p. 14983686.
94. Y. Yin, K. E. Stecke, and D. Li, "The evolution of production systems from Industry 2.0 through Industry 4.0," Int J Prod Res, 2018.
95. Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2022). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 1-17.
96. Seralathan, Y., Oh, T. T., Jadhav, S., Myers, J., Jeong, J. P., Kim, Y. H., & Kim, J. N. (2018, February). IoT security vulnerability: A case study of a Web camera. In 2018 20th International Conference on Advanced Communication Technology (ICACT) (pp. 172-177). IEEE.
97. De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-capable IoT malwares: Comparative analysis and Mirai investigation. Security and Communication Networks, 2018, 1-30.
98. Kambourakis, G., Kolias, C., & Stavrou, A. (2017, October). The mirai botnet and the iot zombie armies. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 267-272). IEEE.
99. Su, J., Vasconcellos, D. V., Prasad, S., Sgandurra, D., Feng, Y., & Sakurai, K. (2018, July). Lightweight classification of IoT malware based on image recognition. In 2018 IEEE 42Nd annual computer software and applications conference (COMPSAC) (Vol. 2, pp. 664-669). IEEE.
100. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.
101. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016, August). Internet of Things (IoT): Taxonomy of security attacks. In 2016 3rd international conference on electronic design (ICED) (pp. 321-326). IEEE.
102. Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, 50(2), 76-79.
103. Trnka, M., Cerny, T., & Stickney, N. (2018). Survey of Authentication and Authorization for the Internet of Things. Security and Communication Networks, 2018.

104. Santoso, F. K., & Vun, N. C. (2015, June). Securing IoT for smart home system. In 2015 international symposium on consumer electronics (ISCE) (pp. 1-2). IEEE.
105. Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. Mobile networks and applications, 24, 796-809.
106. Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 23(2), 1020-1047.
107. Salman, T., & Jain, R. (2017). Networking protocols and standards for internet of things. Internet of things and data analytics handbook, 215-238.
108. Pal, A., Rath, H. K., Shailendra, S., & Bhattacharyya, A. (2018). IoT standardization: The road ahead. Internet of Things-Technology, Applications and Standardization, 53-74.
109. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future generation computer systems, 56, 684-700.
110. Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustainable Computing: Informatics and Systems, 19, 174-184.
111. Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, 1(2), 1-7.
112. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115.
113. Biswas, A. R., & Giaffreda, R. (2014, March). IoT and cloud convergence: Opportunities and challenges. In 2014 IEEE World Forum on Internet of Things (WF-IoT) (pp. 375-376). IEEE.

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.