National Journal of Antennas and Propagation
RESEARCH ARTICLE
National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 6, No. 1, 2024 (pp. 13-22)
WWW.ANTENNAJOURNAL.COM

The Past and Future Trends in IoT Research

Waleed S. Alnumay
Computer Science Department, Riyadh Community College, King Saud University, Riyadh, Saudi Arabia

KEYWORDS:
Internet of Things,
IoT,
Past and future trends,
Review

ARTICLE HISTORY:
Received 04.02.2024
Revised 13.04.2024
Accepted 21.05.2024

DOI:
https://doi.org/10.31838/NJAP/06.01.03

Abstract

The Internet of Things (IoT) has been a rapidly developing field since its inception in 1982. In order to assess the past and future trends in IoT research, a search was conducted on Google Scholar which yielded 25 papers. These papers were then analyzed and discussed, leading to the conclusion that IoT is not only here to stay, but also continuously evolving. This can be seen in the advancements in technology, applications, areas of use, benefits, problems, and challenges. It is expected that this pattern of development will continue in the future, with the emergence of new technologies, applications, software, and areas of use. However, as with any other field, there will be barriers and challenges that need to be overcome at each stage of progress. Furthermore, there is immense potential to integrate IoT with Artificial Intelligence (AI), leading to even more innovative and efficient applications. Overall, the future of IoT research looks promising, with continued growth and advancements in various aspects of the field.

Author's e-mail: wnumay@ksu.edu.sa

How to cite this article: Alnumay WS. The Past and Future Trends in IoT Research, National Journal of Antennas and Propagation, Vol. 6, No. 1, 2024 (pp. 13-22)

Introduction

A strong cloud computing framework, backed up by a seamless blending of sensors and actuators with the environment around us, is making IoT a reality. IoT is expanding from smart wearables to smart cities, domestic life to industries. According to Gartner Inc., the IoT will include 26 billion units installed by 2020. The trending IoT applications are smart security solutions, smart home automation, smart health care, and smart wearables. By the near future, its application to a city's transportation system or smart power grids will be visible (Saha, et al., 2017).

Some of the recent trends in IoT are edge computing, 5G connectivity, artificial intelligence, IoT in healthcare, new sensor research, and IoT as a service. Despite the rapid growth and potential of IoT, research in this field is still relatively new and constantly evolving. With its increasing applications in various aspects of daily life, it is important to understand the past and future trends in IoT research.

One of the major trends in IoT research is edge computing, which involves processing and analyzing data at the edge of the network, closer to where it is generated. This approach reduces latency and saves bandwidth, making it well-suited for IoT applications where real-time analysis is crucial. Similarly, the development of 5G connectivity is expected to further boost the growth of IoT, allowing for more devices to be connected and enabling faster data transmission. Artificial intelligence (AI) has also become an integral part of IoT research, as it enables devices to learn from data and make decisions. With the increasing demand for smarter and more efficient devices, there has been a significant focus on combining IoT with AI. In the healthcare industry, IoT is transforming the way healthcare services are delivered. From remote patient monitoring to real-time data tracking for better diagnosis and treatment, IoT has the potential to improve the quality of healthcare services while reducing costs.

This paper aims to provide an in-depth analysis of these trends and their impact on the future of IoT research. By examining the past and present of IoT research, we hope to provide valuable insights and predictions for future research directions in this rapidly advancing field. This review is a simple exploratory qualitative research aimed at evaluating the status of IoT research.

Methodology & Results

Methods

For this paper, the method of search used was a simple search and selection of papers using Google Scholar. This method was chosen as it allows for a wide range of publications to be considered, and it is a commonly used tool for conducting research. Using the keyword

"IoT research", 25 papers were identified and selected for further analysis and discussion. The papers were then categorized into different sub-topics within IoT research, such as technological advancements, applications, challenges, and future directions. The papers were then thoroughly reviewed and analyzed to identify common themes and trends within the field. The results of this analysis were then discussed in the subsequent section, providing an in-depth understanding of the past and future trends in IoT research. Additionally, some broad quantitative trends, such as the number of publications per year or the most commonly researched topics, were also examined in the discussion section. This comprehensive approach allows for a thorough understanding of the current state and future directions of IoT research.

Results

From a bibliometric study of the literature published during 2000-2019, by Wang, et al. (2021) the mainstream studies focused on IoT security (algorithms), wireless sensor networks, IoT management, IoT challenges and privacy.

Some of the recent trends in IoT research were discussed by Vyas, et al. (2015). The advances in computer hardware, and devices of embedded systems, networking, display, control, and software enhancements etc. have highly supported IoT to grow slowly and steadily. More advanced and universal computation, connectivity, and data storage have led to an explosion of IoT-based application solutions in many areas. The basic pillars of IoT are anything identifiable anytime and anywhere, anything can communicate at anytime and anywhere, and anything interacts anywhere and at anytime (Fig 1). Thus, smart objects are physical entities possessing a unique identity, having some basic computing abilities, and being capable of sensing physical properties like light, sound, and temperature.

The various computational areas of IoT are given in Fig 2.

Fig.2 shows that there is practically no area in which IoT is not useful.

The worldwide nature of IoT networks consisting of interconnected objects uniquely addressable, based on standard communication protocols implies several heterogeneous objects involved. From the perspective of IoT, semantic orientation functions as a solution to the challenges of the object's uniqueness and the representation and storing of the exchanged information. Several visions about IoT can co-exist, as can be seen in Fig 3.

IoT can be considered from three perspectives: the internet perspective, the things perspective, and the semantic perspective. Various visions exist for each of them. Fig 3 shows that the maximum visions occur with

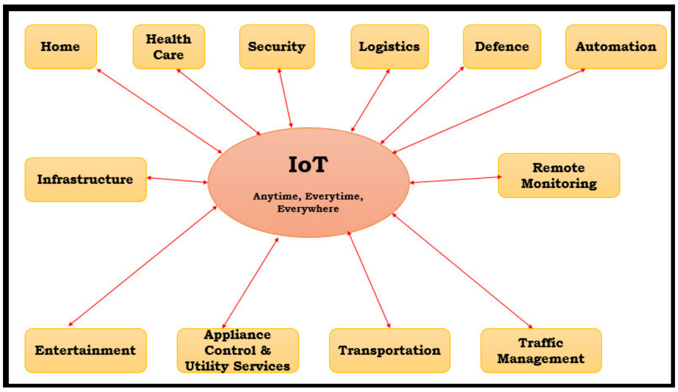

Fig. 2: The different areas in which IoT is useful (Vyas, et al., 2015)

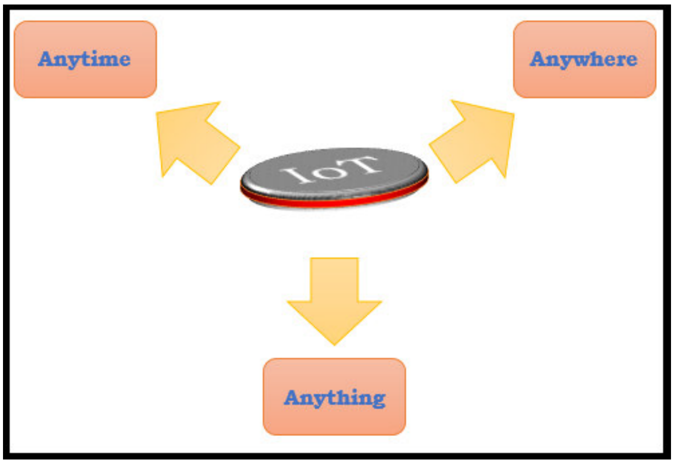

Fig. 1: The three basic pillars of IoT (Vyas, et al., 2015).

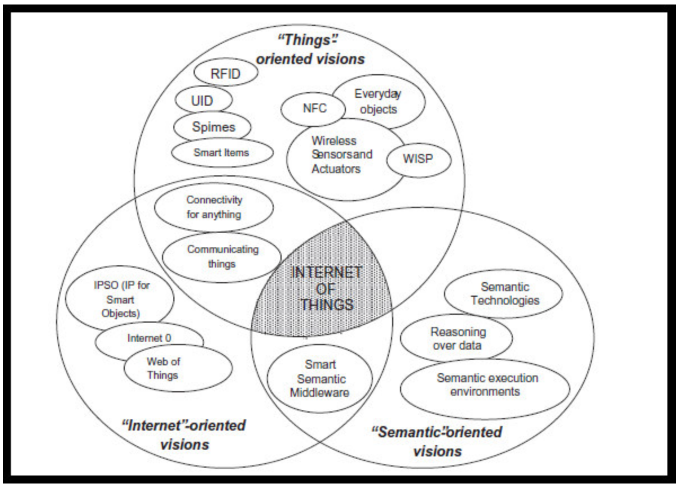

Fig. 3: Various visions of co-existing IoT (Vyas, et al., 2015).

the things perspective. As has been shown in Fig 3, the three perspectives converge to become IoT.

A Gartner hype cycle of emerging was provided by the authors (Fig 4). As can be seen, it was forecasted in 2011 that IoT will be almost fully adopted by the market with cost-efficient solutions. By 2021, IoT had almost achieved this status. It is further developing into AI applications now to support IoT.

The core application areas of IoT are as given in Fig 5.

The core functional areas are transportation and logistics, healthcare, smart environments, personal and social life, and futuristic areas. Surprisingly, sectors like industry, education, and tourism/hospitality sectors, which contribute substantially to the GDP of nations, are not included. The authors have identified a few future research areas, most of which are already being researched now.

Shafique, et al. (2020) noted that 5G-IoT reviewed the key enabling technologies for ubiquitous deployment of the IoT technology. IoT vision is anytime, anywhere, anything. Generally, IoT has hardware comprising nodes, middleware comprising data storage, analysis, and resource handling, and a presentation layer consisting of different visualisation tools compatible with different platforms for different applications. Many strategies are used to address the high energy requirements of 5G-IoT systems. To handle the large volumes of big IoT data, the use of AI, novel fusion algorithms, state-of-the-art temporal machine learning methods, and neural networks for automated decision-making is suggested. There are many opportunities for IoT across different sectors as given in Fig 6.

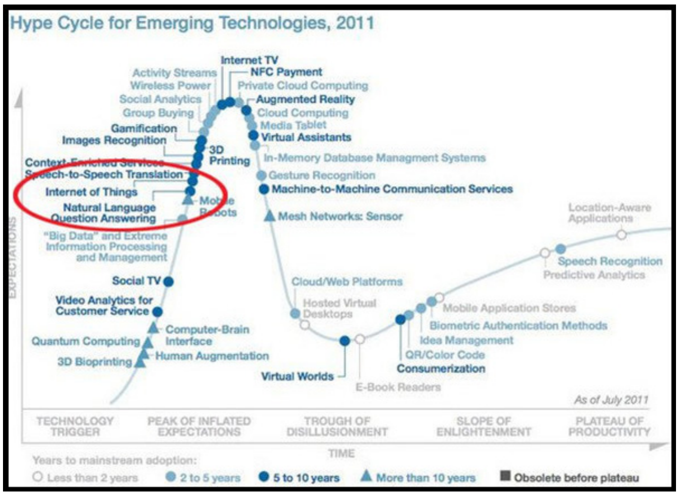

Fig. 4: Gartner hype cycle of emerging technologies (Vyas, et al., 2015).

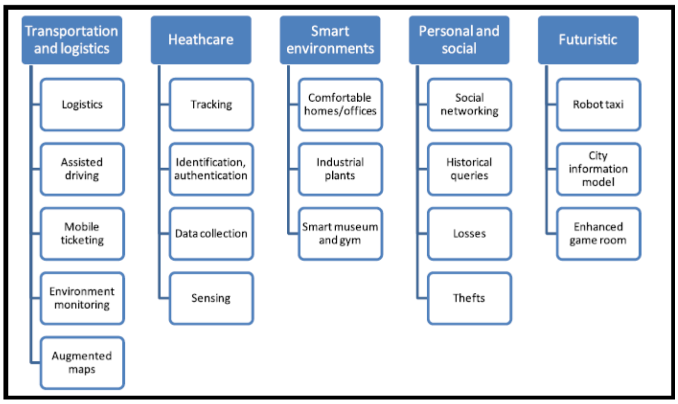

Fig. 5: Core application areas of IoT (Vyas, et al., 2015).

The benefits of IoT include improvement in utilization, minimum user interaction, cost reduction. Proactive maintenance, and new improved services. The features of IoT technologies enabled are carrier aggregation, multiple-input multiple-output (MIMO), massive-MIMO (M-MIMO), coordinated multipoint processing (CoMP), device-to-device (D2D) communications, centralized radio access network (CRAN), software-defined wireless sensor networking (SD-WSN), network function virtualization (NFV) and cognitive radios (CRs). A multi-tier architecture of 5G-IoT is shown in Fig 7.

In this architecture, the front haul, backhaul, peer-to-peer communication, macro and femto cells and end-user equipment have been shown. The emerging use cases of 5G-IoT are driven by developments in artificial intelligence, machine and deep learning, ongoing 5G initiatives, quality of service (QoS) requirements in 5G and issues of its standardisation. An architectural scenario of 5G with AI is provided in Fig 8.

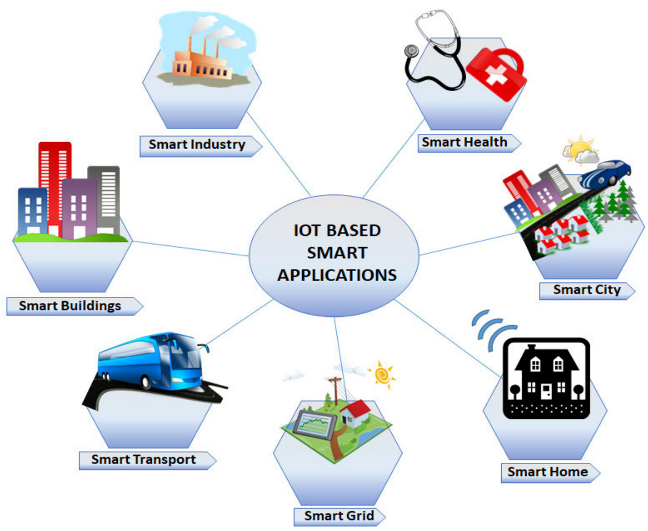

Fig. 6: Some smart applications of IoT (Shafique, et al., 2020).

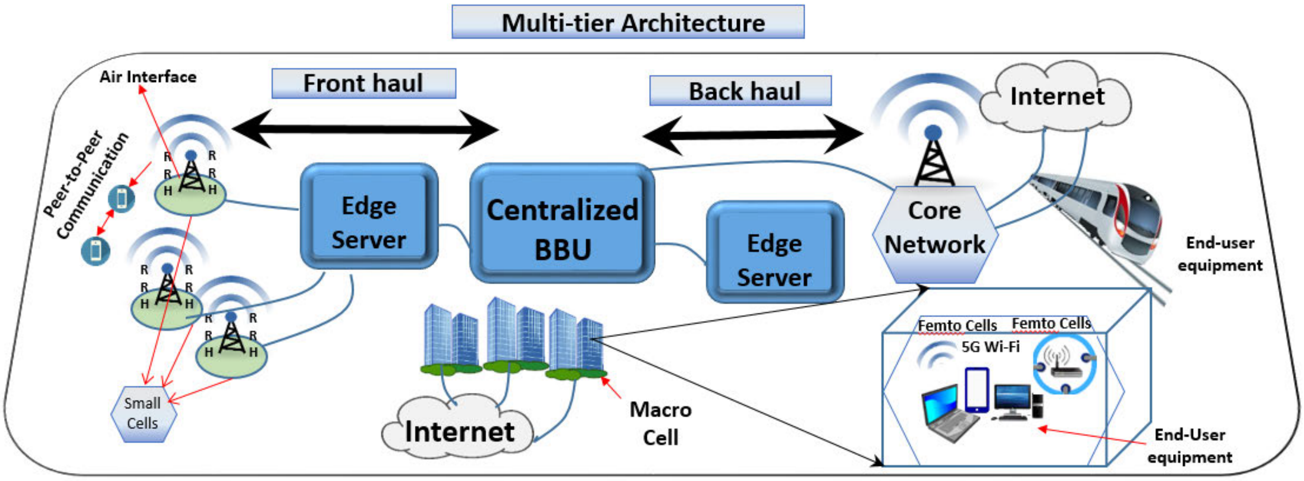

Fig. 7: A multi-tier architecture of 5G-IoT (Shafique, et al., 2020).

In their survey on the IoT, Kassab and Darabkh (2020) included sections on the taxonomy of IoT architecture (IoT layers, Fog layers, cloud computing), distinct spread-spectrum telecommunications techniques such as (DSSS, FHSS, CSS, THSS), IoT layers' protocols (origin, recent, future enhancements), middleware's definition, uses, types and open research challenges, different simulation tools of IoT networks, various types of IoT sensors with recent application areas in IoT, broad and open IoT research challenges before concluding and offering recommendations. The authors have provided many illustrative diagrams, tables, recent trends and future research directions in each section of the paper.

According to Shammar and Zahary (2020), their examination of IoT research material showed a significant emphasis on technology over innovation in business models, highlighting a skewed focus on technological advancements in IoT projects. This raises serious concerns about the potential risks associated with the growth of IoT, particularly in regards to privacy and security. Therefore, industry and government started addressing these concerns. Still, the exact use cases which would have the ability to significantly influence our lives are yet to be known. This makes IoT research exciting.

According to Chin, et al. (2019) the past trend of IoT research had been mainly on manufacturing, supply chain and automotive. The authors divided the IoT research into Phase One 2005–2008 (the devices & connectivity period), Phase Two 2009–2011 (the machine-to-machine period), Phase Three 2012–2014 (the HCI period), and Phase Four 2015 –2017 (the smart period). Some illustrative examples have been tabulated and described.

The challenges discussed by the authors are balancing between the ease of 5G connectivity and security, the flexibility of 5G for different network configurations, the issue of 5G catering to the high density of connected devices and future-proofing 5G. Some research works done for solutions have been discussed.

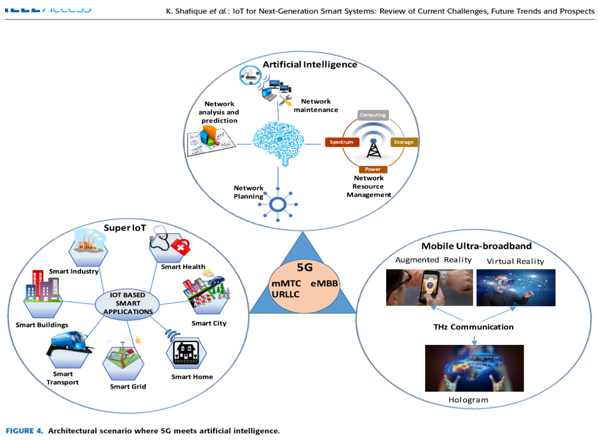

Fig. 8: An architectural scenario of 5G meeting AI (Shafique, et al., 2020).

A systematic review of 417 papers was undertaken by Ghosh, et al. (2021) on IoT research in the construction sector, using a mixed-methods approach consisting of qualitative-scientometric analyses. The review showed research in this sector to be in an initial stage, with a few experts operating in isolation and offering single-point solutions instead of taking an integrated holistic approach. The areas covered were technical areas of smart buildings, smart construction objects and environmental sustainability. Adopting the IoT within the construction industry facilitated high-speed reporting, complete process control, data, explosion leading to deep data analytics, and strict ethical and legal expectations. Key drivers were interoperability, data privacy and security, flexible governance structures, and proper business planning and models.

The emerging trends and potential opportunities for IoT in transportation, logistics, media, shopkeeping, manufacturing, healthcare, energy, home and building were catalogued by Irmak and Bozdal (2018) shown in Fig 9.

IoT, as known now, was born during 2008-2009. However, some early trends pointing towards an IoT concept can be seen since the early 1980s. Semiconductors, sensors and remote access were being used for a long time. The article entitled "The Internet of Things" in Forbes Magazine in 2002 is the first documented use of the term IoT. The first book on the concept was contained in a book, "When Things Start to Think¤ by Neil Gernshenfeld published in 1999. The first academic conference on IoT was held in 2008. A tabulated list of the historical developments of IoT is given in Fig 10. The history has been traced from 1982 when Carnegie Melon University, USA developed an internet-connected coke-vending machine to Tesla developing a self-driving car in 2017, since this paper was published in 2018. Between the two years, many landmark developments of IoT took place in the USA, UK, Australia, South Korea, France, Italy and globally.

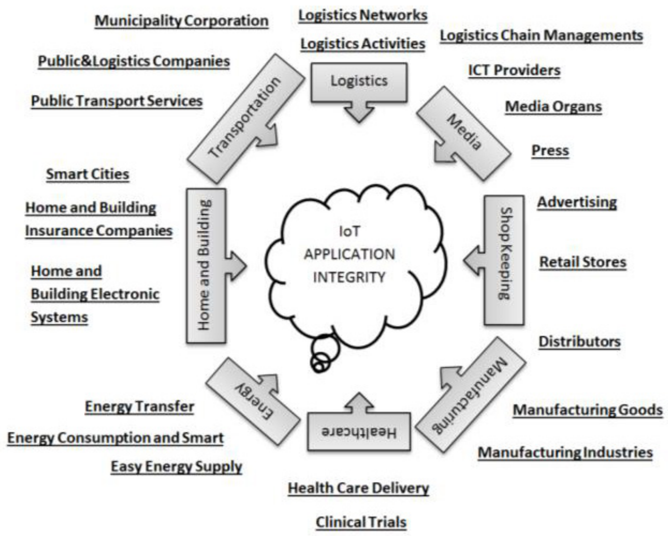

Fig. 9: Emerging trends and potential opportunities of IoT (Irmak & Bozdal, 2018).

Some popular applications of IoT are given in Fig 11. Four types of IoT applications have been listed here. ITU-TY-2060 has two application layers, and two service supports serving different functions. IIC IIRA has four viewpoints about business, usage, functional, and implementation. RAMI 4.0 consists of business, functional, information, communication, integration, and asset components. IOT-A ARM has five models domain, information, functional, communication, and security. Other points are repetitive of the above-discussed aspects.

Table 1. From Its First Glimpses into Today's Trending Topic

Technology	By	Country	Reference	Year
Internet Connected Coke Vending Machine	Carnegie Melon University	USA	[11]	1982
Ubiquitous term was first coined	Mark Weiser	USA	[12]	1988
Deluxe Automatic Radiant Control Toaster	John Romkey and Simon Hacket	Australia	[13]	1990
Tangible Telephone	Scott Brave and Hiroshii Ishii	USA	[14]	1998
First IoT touch, Water Fountain	Mark Weiser	USA	[12]	1998
IoT term is first coined	Kevin Ashton	UK	[1]	1999
First book was written about IoT	Neil Gershenfeld	USA	[15]	1999
EPC development	Auto-ID Labs	USA	[16]	2003
First Internet of Refrigerator Plans	LG	South Korea	[17]	2000
The Ambient ORB	David Rose	USA	[18]	2002
IoT term first used in Main Stream Publications	US Department of defense	USA	[19]	2003
WiFi Enabled Artificial Rabbit, Nabaztag	Rafi Haladjian and Olivier Mével	France	[20]	2005
ARDUINO Microcontroller invented	Interaction Design Institute Ivrea	Italy	[21]	2005
IPSO Alliance, use of IP in networks of Smart Objects	IPSO Alliance	Global	[22]	2008
Use of White Space Spectrum	Federal Communications Commisions	USA	[23]	2008
IoT accepted as Disruptive Civil technologies	US National Intelligence Council	Global	[24]	2008
More objects connected to internet than people	CISCO Business Solutions Group	Global	[2]	2009
IPv6 Public Launch	Internet Engineering Task Force	Global	[24]	2011
INTEL launched Internet of Things Solution Groups	INTEL	USA	[25]	2013
A Pilot Smart City Implementation, Padova Smart City	University of Padova	Italy	[26]	2014
Self-driving Car	TESLA's Elon Musk	USA	[27]	2017

Figure 10 The historical development of IoT concepts (Irmak & Bozdal, 2018).

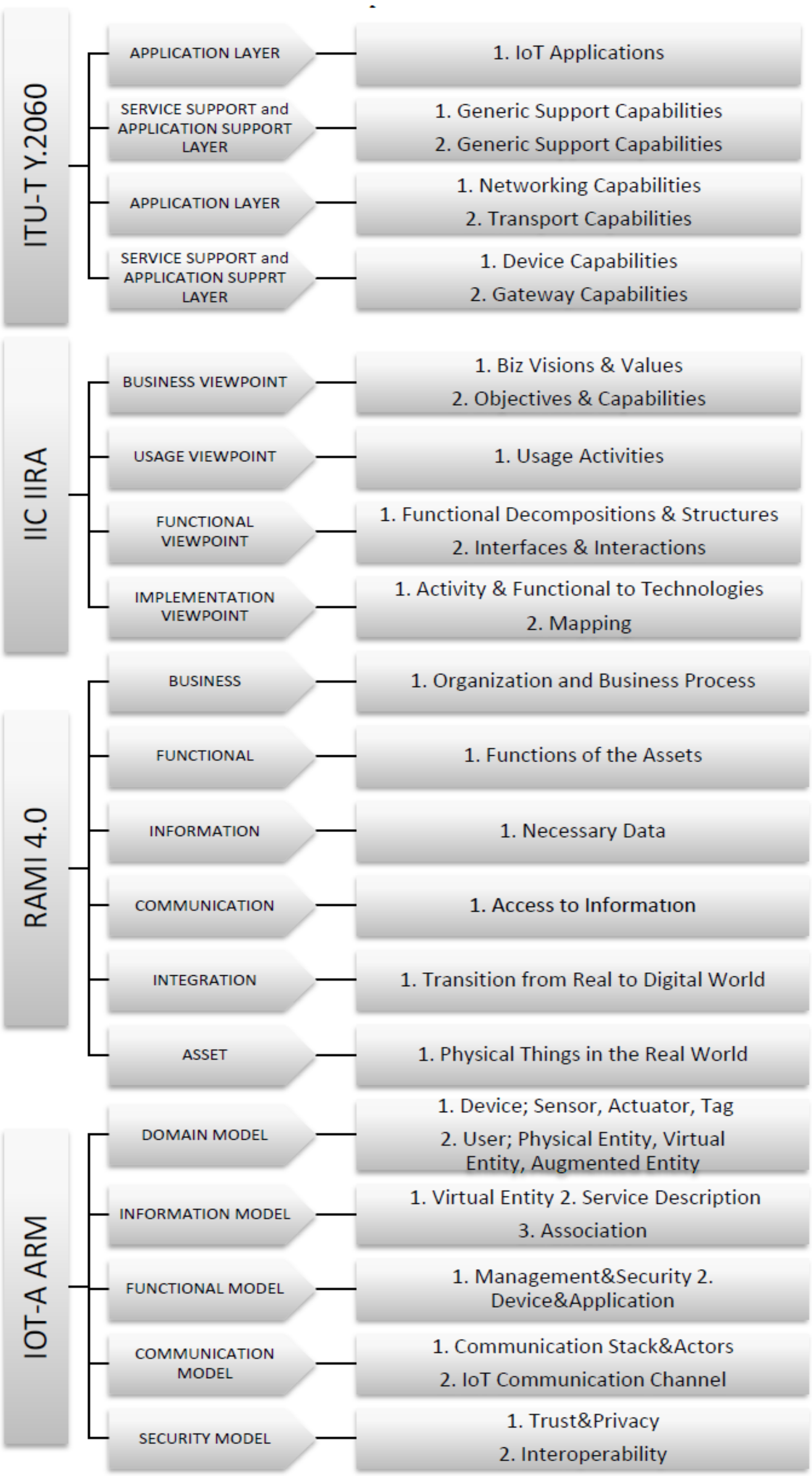

Fig. 11: Some popular applications of IoT (Irmak & Bozdal, 2018).

After analysing 300 non-technical articles, Lee, et al. (2017) discovered a serious lack of a multidisciplinary and social science approach, and systematic qualitative and tangible research. Some suggestions for future research have been given.

A review by Miraz, et al. (2018) observed that one notable characteristic of IoT is that it represents various electrical and electronic devices of various sizes and capabilities directly connected to the internet. But it excludes those involved in connections to human beings (the traditional internet). IoT is a network of networks. Internet of Everything (IoE) has four pillars consisting of people, data, process and things (Fig 12). IoT is only composed of things.

In the Internet of Nano-Things (IoNT), the IoE concept is extended to its full implementation by incorporating nano-sensors in diverse objects using nano-networks. An example of this in a medical application is shown in Fig 13. In this example, nano-sensors are attached to clothes and body parts. Phone surface sensors and nano-sensors for environmental monitoring are also shown.

The challenges discussed are the same as the ones discussed above. The authors listed some future research trends.

A survey of literature by Gharami, et al. (2019) revealed several applications of IoT in the practical world. Some examples of IoT applications discussed were commonly experienced problems. The utility of IoT in smart cities, smart doorbells, smart medicinal bottles, smart clothes, and smart homes was discussed with illustrations.

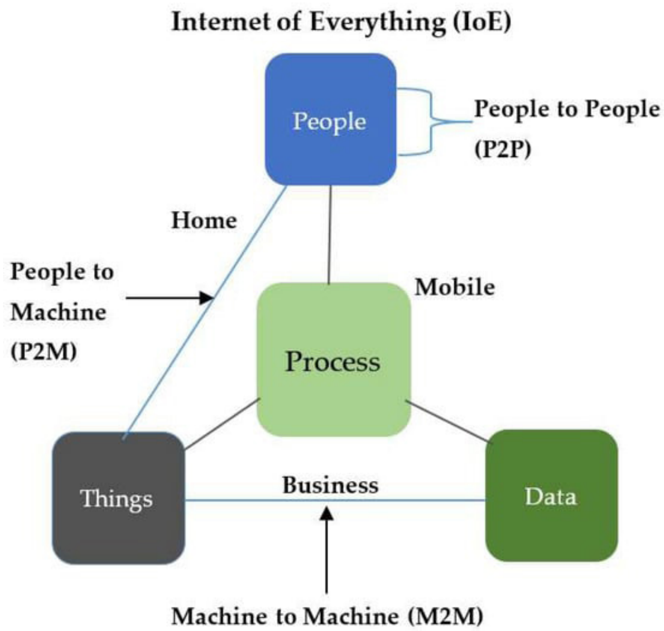

Fig. 12: Internet of Everything architecture (Miraz, et al., 2018).

A classification with examples of IoT applications was discussed and illustrated by Kawamoto, et al. (2014) according to the scale of things and level of networks. The authors discussed research works on IoNT, the internet of Wi-Fi-enabled things, and global scaled IoT. An example of the co-existence of different sizes of IoT systems was also illustrated and discussed. A case study of the Tsunami detection system was illustrated and discussed. Future research prospects included integrated IoT systems, requirements for the next-generation IoT systems, network-scale-based security systems, and data processing.

Many future industries will have to rely on IoT. This technology can increase the productivity and efficiency of industries through intelligent integration of sensors, wireless communications, computing techniques, and data analytics. However, IoT applications need reliable data transmission. Future opportunities of IoT depend on machine learning technologies, 6G communications, and blockchain-enabled security (Khan, et al., 2021).

In Mohamed's (2020) study, a variety of documents concerning the use of IoT in diverse fields were examined. The researchers observed that the widespread use of intelligent and capable devices within communication networks has facilitated the emergence of IoT as a novel approach to internet connectivity. By incorporating various wireless technologies, such as Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID),

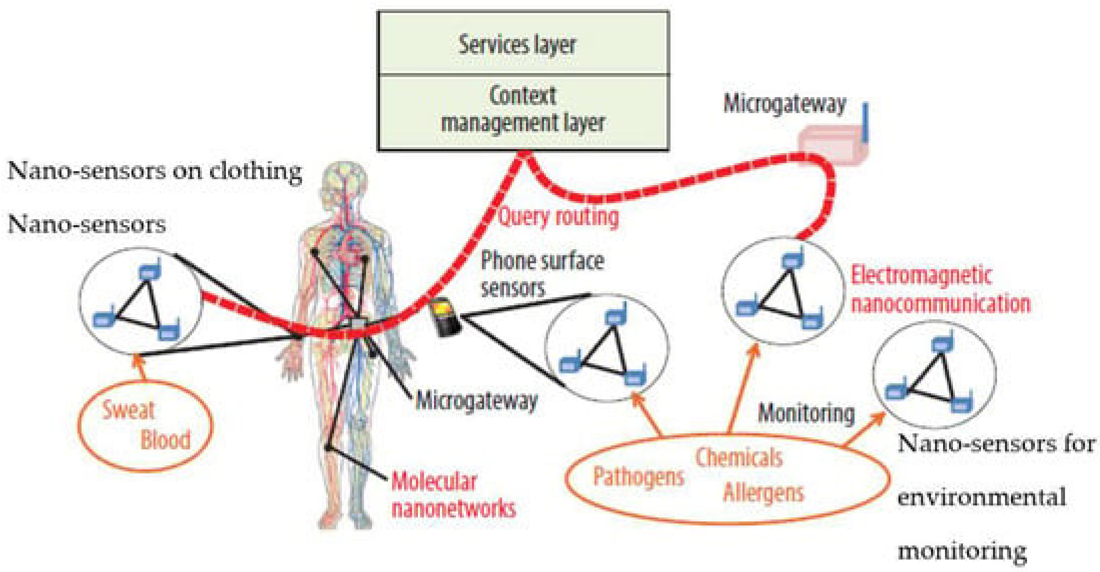

Fig. 13: A medical example of IoNT (Miraz, et al., 2018).

Near Field Communication (NFC), and barcodes, IoT has revolutionized the internet into a seamlessly integrated platform. Additionally, the study also addressed the potential application of IoT in agriculture in the coming years.

Factory of the Future and Industry 4.0 visualise knowledge-intensive intelligent industrial environments in which smart personalised products are produced using smart processes. Such disruptive paradigms of manufacturing are strongly based on IoT and Cyber-Physical Systems. Cyber-Physical Systems will monitor, analyse and automate processes. This leads to the transformation of production and logistics into smart factory environments. Such smart environments have big data capabilities, cloud services and smart tools for decision-making leading to increased productivity and efficiency (Preuveneers & Ilie-Zudor, 2017).

According to Din, et al. (2018) review, previous research on the Internet of Things (IoT) has highlighted several key technologies that facilitate its operation, such as fog computing, wireless sensor networks, data mining, context awareness, real-time analytics, virtual reality, and cellular communications.

By incorporating systems, software, cloud technology, and intelligent sensors into a unified system, the Internet of Multimedia Things (IoMT) facilitates a seamless integration process. This platform can handle both scalar and multimedia data effectively. However, the inclusion of smart sensors in these networks brings about various security challenges. In a recent study, Jan, et al. (2021) examined the potential of combining blockchain technology with IoMT and multimedia-enabled blockchain platforms to address security concerns in large-scale business projects. The healthcare industry was used as a case study to validate a theoretical framework in which security and blockchain function as enablers of services.

According to Park and Park (2020), the future trends of IoT research include clustering, Hyperledger Fabric and digital evidence management based on this, data, security, machine vision, CNN and using it as a basis for voting and ensemble systems, IoT technology, resource management of 5G mobile networks, stay point spatial clustering-based technology, aircraft recognition using machine vision, hierarchical semantic clipping and sentence extraction, N-step sliding recursion formula, routing protocol for improving the lifetime of a wireless sensor network, fault diagnosis of wind power generator blade, variant malware detection techniques and application of blockchain in multiple fields of financial services.

During 2009-2020, the focus of IoT research was certain aspects of IoT security. Based on this observation and keyword clusters, trends and topics, Lee and Lee (2021) proposed future research on the development of a secure decentralized framework integrating edge computing, ML-based SDN, and blockchain, and research on vehicles and UAVs as smart M-IoT objects.

A bibliometric and systematic review of the IoT research papers by Furstenau, et al. (2023) identified 11 themes dealt with in these papers. They were authentication, cloud computing, industry 4.0, 6lowpan, smart city, machine learning, platform, interoperability, distributed system and SOA. A thematic evolution structure of IoT components was also given. The main challenges, limitations and difficulties of IoT are privacy and security issues, technology, communication, job, legal and regulatory, and culture. Suggestions for future research are not very specific.

A review of current IoT standards and protocols by Rachit and Ragiri (2021) led to the identification of security risks of the current IoT system, novel security protocols, and security projects offered in recent years. The review showed the need for standardization at the communication and data audit level, which exposes the hardware, software, and data to various threats and attacks. The authors described with diagrams or tables the multilayered IoT architecture, classification of attacks on IoT systems in various ways, challenges to security, and a comparative analysis of IoT protocols. A similar review of IoT security issues was provided by Harbi, et al. (2021) with tables and diagrams.

Among the innovative techniques tested for the future IoT (FIoT), the extraction of data and its transformation into knowledge from the sensing layer to the application layer is a critical issue. An intelligent data management framework based on swarm optimisation has been proposed for this purpose (Tsai, et al., 2014).

In the case of smart cities, IoT facilitates the creation of smart mobility, healthcare, energy, and civil infrastructure using a massive worldwide network of interconnected physical objects embedded with electronics, software, sensors, and network connectivity. Research to strengthen these applications for smart city facilities will mark the future trend of IoT (Alavi, et al., 2018).

Information security concepts have been changing periodically due to frequent changes in technology and the market. In the previous ten years, there were concerns about privacy in cloud computing or third-party public clouds. But now using a cloud service is widely accepted as adequate security is assured by cloud providers. Business organisations are satisfied with the benefits of low cost and elasticity offered by the cloud. Earlier, there was no protocol for developing IoT technology. Now the Message Queuing Telemetry Transport (MQTT) is a widely accepted standard protocol. IP addresses were not different between IoT and other computer processes. Now attempts are made to differentiate them. The past to future trends of IoT research can be explained in terms of generations. Thus, in the first generation, IoT services were considered complex limiting their use. Hence, the developers only had challenges. Privacy issues were common in the early years. The second generation refers to the current generation. A large number of cloud-based IoT platforms offer infrastructure and libraries. Therefore, both established and new developers find it easier to implement IoT using these platforms. Demand for IoT services is rapidly increasing; hence faster development and delivery of products is important. When third-party services become well-known, developers are forced to use the same standards for compatibility with the current libraries. People are now more familiar with IoT and it is used widely, although some privacy issues still exist. The third or future generation will focus on value creation for business organizations. The use of IoT will expand to other areas. Rich data from device transactions will be centrally stored. These data can be analysed by a service provider to create value for the business and improve productivity. Privacy of customer data will be an issue (Vorakulpipat, et al., 2018).

Discussion

This review was conducted to quickly assess the past and future trends in IoT research. Being a novel topic, several papers were identified discussing various aspects of IoT technology, applications, standards, challenges, and problems.

The 25 reviewed papers displayed IoT as a revolutionary technology still evolving and growing to its full potential. The anytime, anywhere anything characteristics of IoT lead to many applications in many areas (Vyas et al., 2015). Many heterogeneous objects connected to it were displayed by Vyas et al. (2015). The past, present and future trends were clear from the Gartner-type diagram. IoT can be used beneficially in many smart applications (Shafique et al., 2020). The earlier three-layered structure of IoT has become a multilayered structure. Some papers discussed scenarios of past and future IoT applications. As was observed by Irmak & Bozdal, (2018), many opportunities still exist for using IoT in diverse areas. These authors traced the historical trends of IoT from 1982 to 2017. The concept of IoT has been extended to the Internet of Everything (IoE), Internet of Nano-Things (IoNT), Internet of Multimedia Things (IoMT) and future IoT (FIoT). There is scope to integrate artificial intelligence into IoT applications. Future research will focus on this area also.

Despite all these developments and benefits, the challenges related to privacy and security of the data in the cloud have not been fully solved yet. This is particularly true when businesses use customer data from the cloud to plan their marketing strategies. The use of deidentified data is a method used by researchers, but there is no indication that businesses are doing it.

Overall, the review achieved its aim by highlighting the past and future trends in various aspects of IoT in various applications and some problems and challenges continuing from the past.

Conclusion

IoT has been developing rapidly since its first use in 1982. IoT is here to stay now and forever. This rapid development can be seen concerning the technology, applications, areas, benefits, problems and challenges. Some of these will continue in the future. New technologies, applications, software and areas of use are emerging and will continue in the future. On the way to progress, gates of barriers and challenges will need to be solved at each stage. The scope to integrate AI into IoT applications is tremendous.

References

1. Alavi, A. H., Jiao, P., Buttlar, W. G. & Lajnef, N., 2018. Internet of Things-enabled smart cities: State-of-the-art and future trends. *Measurement*, Volume 129, pp. 589-606.
2. Chin, J., Callaghan, V. & Allouch, S. B., 2019. The Internet-of-Things: Reflections on the past, present and future from a user-centered and smart environment perspective. *Journal of Ambient Intelligence and Smart Environments*, 11(1), pp. 45-69.
3. Din, I. U. et al., 2018. The Internet of Things: A review of enabled technologies and future challenges. *Ieee Access*, Volume 7, pp. 7606-7640.
4. Furstenau, L. B. et al., 2023. Internet of things: Conceptual network structure, main challenges and future directions. *Digital Communications and Networks*, 9(3), pp. 677-687.
5. Gharami, S., Prabadevi, B. & Bhimnath, A., 2019. Semantic analysis-internet of things, study of past, present and future of IoT. *Electronic Government, an International Journal*, 15(2), pp. 144-165.

6. Ghosh, A., Edwards, D. J. & Hosseini, M. R., 2021. Patterns and trends in Internet of Things (IoT) research: future applications in the construction industry. *Engineering, Construction and Architectural Management,* 28(2), pp. 457-481.
7. Harbi, Y. Z. A., Refoufi, A. & Harous, S., 2021. Recent security trends in internet of things: A comprehensive survey. *IEEE Access,* Volume 9, pp. 113292-113314.
8. Irmak, E. & Bozdal, M., 2018. Internet of Things (IoT): The most up-to-date challenges, architectures, emerging trends and potential opportunities. *International Journal of Computer Applications,* 179(40), pp. 20-27.
9. Jan, M. A. et al., 2021. Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *Journal of Network and Computer Applications,* Volume 175, p. 102918.
10. Kassab, W. & Darabkh, K. A., 2020. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications,* Volume 163, p. 102663.
11. Kawamoto, Y. et al., 2014. Internet of things (IoT): Present state and future prospects. *IEICE TRANSACTIONS on Information and Systems,* 97(10), pp. 2568-2575.
12. Khan, M. Z. et al., 2021. Reliable Internet of Things: Challenges and future trends. *Electronics,* 10(19), p. 2377.
13. Lee, J. Y. & Lee, J., 2021. Current research trends in IoT security: a systematic mapping study. *Mobile Information Systems,* p. Article ID 8847099.
14. Lee, S.-E., Choi, M. & Kim, S., 2017. How and what to study about IoT: Research trends and future directions from the perspective of social science. *Telecommunications Policy,* 41(10), pp. 1056-1067.
15. Miraz, M. H., Ali, M., Excell, P. S. & Picking, R., 2018. Internet of nano-things, things and everything: future growth trends. *Future Internet,* 10(8), p. 68.
16. Mohamed, M., 2020. A comparative study on Internet of things (IoT): Frameworks, tools, applications and future directions.. *Journal of Intelligent Systems and Internet of Things,* 1(1), pp. 13-39.
17. Park, J. S. & Park, J. H., 2020. Future trends of IoT, 5G mobile networks, and AI: challenges, opportunities, and solutions. *Journal of Information Processing Systems,* 16(4), pp. 743-749.
18. Preuveneers, D. & Ilie-Zudor, E., 2017. The intelligent industry of the future: A survey on emerging trends, research challenges and opportunities in Industry 4.0. *Journal of Ambient Intelligence and Smart Environments,* 9(3), pp. 287-298.
19. Rachit, S. B. & Ragiri, P. R., 2021. Security trends in Internet of Things: A survey. *SN Applied Sciences,* Volume 3, p. 121.
20. Saha, H. N., Mandal, A. & Sinha, A., 2017. *Recent trends in the Internet of Things.* s.l., IEEE.
21. Shafique, K. et al., 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,* Volume 8, pp. 23022-23040.
22. Shammar, E. A. & Zahary, A. T., 2020. The Internet of Things (IoT): a survey of techniques, operating systems, and trends. *Library Hi Tech,* 38(1), pp. 5-66.
23. Tsai, C.-W., Lai, C.-F. & Vasilakos, A. V., 2014. Future internet of things: open issues and challenges. *Wireless Networks,* Volume 20, pp. 2201-2217.
24. Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P. & Hai, H. D., 2018. *Recent challenges, trends, and concerns related to IoT security: An evolutionary study.* s.l., IEEE, pp. 405-410.
25. Vyas, D. A., Bhatt, D. & Jha, D., 2015. IoT: trends, challenges and future scope. *International Journal of Computer Science and Communication,* 7(1), pp. 186-197.
26. Wang, J., Lim, M. K., Wang, C. & Tseng, M.-L., 2021. The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering,* Volume 155, p. 107174.