A Survey on Internet of Things: Concepts, Technologies, and Applications

COMP4342 Mobile Computing Assignment

ZHOU Siyu 21094655D

Abstract

The Internet of Things (IoT) has developed as an important 21st-century technology trend, connecting physical items and gadgets to the internet, and enabling a wide range of applications and services. This survey seeks to provide a complete overview of Internet of Things principles, technologies, and applications, highlighting important accomplishments and obstacles in this field. The survey starts by defining the core concepts and principles behind the Internet of Things, such as the concept of networked devices, sensor networks, and communication protocols. Following that, it delves into the many technologies that enable IoT connectivity, such as wireless communication protocols, edge computing, and cloud computing. In addition, the survey analyzes the many IoT application fields, such as smart cities, healthcare, agriculture, transportation, and industrial automation. Finally, it addresses the major obstacles and concerns related to IoT, such as data management, interoperability, and scalability. This survey intends to facilitate a deeper understanding of IoT's potential, benefits, and ramifications for numerous industries and communities by offering a complete overview of the technology.

Content

Introduction

The Internet of Things (IoT) refers to “a network of physical devices, vehicles, appliances and other physical objects that are embedded with sensors, software, and network connectivity that allows them to collect and share data” [1]. The Internet of Things (IoT) has developed as an important 21st-century technology trend, connecting physical items to the internet, and allowed a wide range of applications and services.

The survey will provide a comprehensive introduction to IoT, describing its fundamental concepts and principles (the idea of interconnected devices, sensor networks, and communication protocols), demonstrating the architectures of IoT systems and the technologies used, identifying, and describing major challenges faced by IoT, such as security, privacy. Then discuss potential areas for further research and extension of current works.

Review

Concept of Internet of Things

The term “Internet of Things” was first used in 1999 by Kevin Ashton during a Procter and Gamble presentation [2]. He discussed the potential prosperity after implementing RFID technology in products management in this presentation. By integrating the products with devices, people can get relevant information (status, tracking, etc.).

Products could provide information about themselves, but much more efficiently [3]. The Internet of Things now includes intelligent sensing and wireless communication technologies. And as depicted in Figure 1, the evolution of IoT can be divided into many phases.

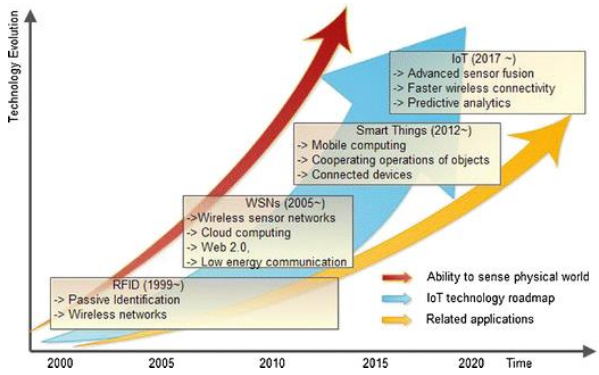

Figure 1 The Evolution of the IoT [4]

Emerging wireless sensory technologies have considerably expanded device sensing capabilities. IoT involves a variety of technologies, including barcodes, RFID, NFC, cloud computing, etc. The evolution of these technologies introduces innovative technologies into the IoT. The concepts of IoT can be altered depending on which technologies are used. The core of IoT is that things in IoT may be identified by unique identifiers and can communicate data.

Different Types of IoT Architectures

One essential requirement of an IoT is that every item in network is interconnected, so that IoT system architecture is required to link the real and virtual worlds. Also, IoT architecture should be adaptable to allow devices to interact with other things dynamically and support clear event transmission.

Several factors contribute to the design of IoT architecture, including “networking, communication, business models and procedures, and security” [5], etc. The IoT architecture must have the following characteristics [6]:

- **Distributivity:** Data may be collected from several sources and distributed handled by multiple entities.
- **Interoperability:** Devices from many suppliers will need to work together to achieve shared goals.
- **Scalability:** The systems should be able to deal with unprecedented volume of created data without degrading performance.
- **Scarcity of resources:** The system will be operated with few resources.
- **Security: The** system should not allow unauthorized access.

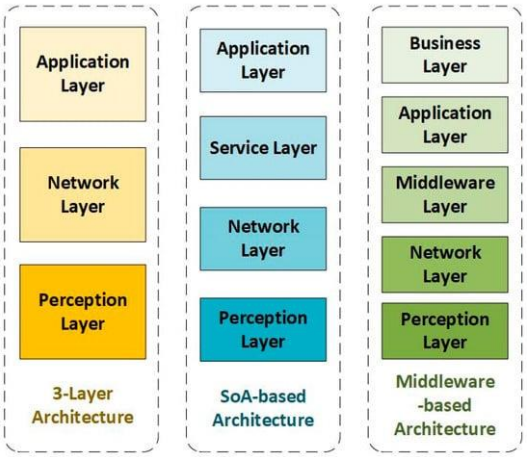

Figure 2 IoT Architectures [3]

Three-Level Architectures

1. Perception Layer

This Layer represents collecting and processing information from the physical level. The IoT is based on smart objects, functionally intelligent objects like refrigerators, televisions, or other simple devices with senser and computing chips. These smart objects in general have the following attributes [7] [8].

- **Communications:** The objects can be interconnected. Also can update data and access services with Internet.
- **Identification:** The objects must be identified uniquely.
- **Addressability:** The objects can be directly addressed.
- **Sensing:** The objects could gather information through the environment and employ it.

- **Processing information:** the object can process calculations with the sensor and drive the actuator.

Various hardware platforms have these attributes, such as Arduino, RaspberryPi, etc.

2. Network Layer

The Network Layer supports the wired or wireless connection to transport data from the hardware to the application layer. It also utilizes some protocols. For example, IPv6 protocol evolves for solving addressing problems because IPv4 protocol addresses run out. But it was invented for wired networks. When it comes to wireless networks, the 6LoWPAN protocol was invented [9]. In this layer, one of the most important protocols is the wireless protocols, because wireless sensor requires less material and human resources.

3. Application Layer

As for the application layer, it is utilized to provide service. The data from the network layer are collected, leaked, and handled, etc. Then the data will be available for applications, such as smart wearable, smart home, etc. The technologies used nowadays to handle the enormous amount of info provided are cloud computing and edge computing. IoT applications always use commercial platforms like Amazon AWS, Microsoft Azure, etc. [3].

Service-oriented Architecture

In IoT, service-oriented architecture (SoA) might be crucial for the service providers and users, which “can ensure interoperability among heterogeneous devices in multiple ways” [4] [10] [11]. SoA is intended to facilitate services with hardware and software components mentioned above. SoA could be readily incorporated into IoT design, adding another service layer, which provides services to the application layer.

The Service Layer manages the service required by users or applications with some service functions such as service discovery (discover service request), service composition (integrate service to get requests efficiently), and service interface (support interactions) [3].

Middleware Architecture

Middleware-based IoT architecture assists in building software more efficiently. The middleware layer acts as the connection between data, applications, and users, in particular, performs essential tasks like collecting and data filtration obtained from hardware gadgets, conducting information discovery, and giving access control to devices for applications [3].

Technology in IoT

Identification and tracking technologies

The IoT concept was born based on RFID technology as we mentioned before. A basic RFID system includes an RFID reader and an RFID tag. RFID systems have been widely used in a variety of industries such as logistics and supply, farm management, healthcare, and payment transactions, because of their capability of identifying, tracing, and tracking objects [12] [13]. An RFID system could convey real-time data about objects to suppliers, manufacturers, and retailers. RFID applications in supply chain management, for example, can enhance the management of inventory. Some advantages highlighted include lower labor costs, streamlined corporate procedures, and increased efficiency.

Wireless RFID sensors have not yet been widely available in personal electronics markets, despite the obvious benefits of RFID for tracking and operate common items. Six major difficulties have been identified in the survey [13]. Figure 3 demonstrates an overview of the primary RFID difficulties, which are organized by the RFID components (reader, passive sensor, communication protocol) that they influence [13].

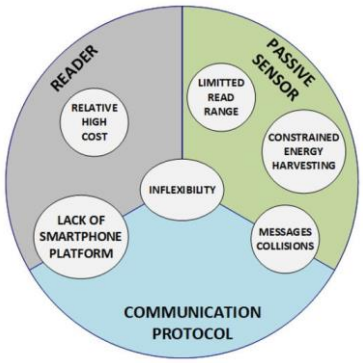

Figure 3 Main Challenges that prevent RFID from becoming pervasive [13]

- **Limited energy harvester and read range:** RFID platforms instrumented cannot operate without sensing data within the reading zone of sensor in the IoT.
- **Sensor responses collisions:** The use of RFID sensors in applications involves a reader and multiple sensors. These sensors can cause collisions when communicating with the reader due to the shared communication channel [13]. This collision problem can result in a waste of energy, increased identification time, and decreased read rate. For sensed data, anti-collision protocols are necessary to diminish the impact.
- **Lack of flexibility:** Currently, RFID tags are not easily being reconfigured (like a black box system) [3], which limits their adaptability in IoT evolvement. The ability to generalize, modularize, and reconfigure sensing nodes/platforms is crucial for their future integration into the IoT architecture. Additionally, commercial RFID readers have limited configuration options and can only support the EPCglobal Class 1 Generation 2 (EPC C1G2) communication standard, preventing the implementation of new protocols for emerging RFID-based sensors [13].
- **Cost:** Commercial RFID readers are expensive comparing to the costs of RFID tags and RFID sensors.

Communication

Hardware devices in IoT need to be well organized and accessible via communication networks, typically through gateways. IoT is a combination of different networks like WSNs, wireless mesh networks, mobile networks, and WLAN [14], which enable complex activities and data exchange. Reliable communication between the gateway and devices is crucial for centralized decision-making. The gateway can run complex algorithms locally and obtain optimal routes and parameter values.

Different devices in IoT have varying capabilities and communication requirements. For example, smartphones have better communication and computation capabilities compared to single-purpose devices like heart rate monitors. Quality of Service (QoS) requirements also differ, including factors like delay, energy consumption, and reliability. Battery-powered devices without efficient energy harvesting techniques focus on minimizing energy use [3], while devices with power supply connections have less critical energy constraints.

The protocols and standards used in IoT include [3]:

- RFID
- NFC, IEEE 802.11(WLAN), IEEE 802.15.4(ZigBee), IEEE.15.1(Bluetooth)
- IETF Low power Wireless Personal Area Networks(6LoWPAN)
- IP technology - IPv6
- Machine to Machine(M2M)

Application of IoT

Industry application (Industry 4.0)

Working conditions (for example, the assistance of a robot) as well as safety and productivity in an industry might be enhanced by incorporating innovative technology into production processes [15].

Smart Agriculture

Farmers could remotely monitor the health and real demands of crops using a network of sensors and actuators in IoT to exploit resources (water, fertilizers, etc.) in an efficient and targeted manner [16].

Smart City

A sensors' network may be utilized for effectively administrate resources supplies, transportation, electric power, garbage collection, etc., thereby reducing pollution and waste while increasing citizen comfort. For example, with intelligent parking management system, residents would save time hunting for a available parking place. With public street lightening management system, lighting can be adjusted based on pedestrian and vehicle traffic, allowing for energy savings.

Smart Healthcare Application

This application could monitor patients' health via electronic devices (may even be implanted inside human) to be able to prevent, diagnose, and treat patients even while they are located far away from the doctor. Furthermore, tracking the healthcare services' demand allows for more efficient investment in certain sectors of healthcare.

Main Challenging Issue

Integrating wireless communications into various applications can be challenging due to their diverse requirements. This includes IoT applications, which connect objects in different environments with unique requirements. However, all wireless sensor networks (WSNs) face usual challenges.

Reliability is essential for nodes to continuously monitor more crucial areas. However, this can lead to unnecessary computations, draining node batteries. Time synchronization and spectrum-sharing techniques are crucial for ensuring data integrity and conserving radio resources.

Energy consumption is another challenge. Nodes must be power efficient, ideally, they should harvest energy efficiently and minimize waste during operations.

Scalability is important as IoT solutions involve numerous smart devices. WSNs must be able to accommodate new nodes, provide Quality of Service (QoS) across heterogeneous devices, and operate for extended periods.

Communication protocols: There are four types of MAC communication strategies, each with its advantages and drawbacks. It is crucial to choose the most suitable strategy based on the specific application's needs. Additionally, WSNs used here need to incorporate Internet functions, with the Internet Protocol (IP) being commonly used for message routing within the wireless network.

Future direction of IoT

In the future, research on IoT may focus on addressing the current challenges and limitations to enhance the capabilities and potential of this technology. These are areas that require future exploration.

1. Security Enhancements: IoT systems and networks become more interconnected and collect sensitive data, ensuring robust security and privacy measures becomes crucial. Additionally, the development of secure and reliable firmware and software update mechanisms is essential to protect IoT devices from potential vulnerabilities.

2. Standardization and Interoperability: To enable seamless communication and integration of devices from different manufacturers and ecosystems, there is a need for standardized protocols and interfaces. Future research should focus on developing

standardization frameworks that enable interoperability between different IoT devices, platforms, and networks, promoting compatibility and ease of deployment for various applications.

3. Energy Efficiency and Sustainability: Energy consumption is a significant concern in IoT, especially for battery-powered devices. Future research should focus on developing energy-efficient algorithms, power management techniques, and energy-harvesting solutions to extend the battery life of IoT devices. Additionally, exploring sustainable power sources, such as solar or kinetic energy, could further enhance the sustainability of IoT systems.

4. Data Analytics and Machine Learning: With the massive amount of data generated by IoT devices, advanced data analytics and machine learning techniques are needed to extract meaningful insights and enable predictive and prescriptive analytics.

Overall, the future direction of research on IoT should revolve around addressing the current limitations while considering the societal impact, security, privacy, interoperability, and sustainability of IoT systems. By solving these challenges, IoT can reach its full potential and revolutionize various industries and sectors.

Conclusion

In conclusion, the Internet of Things (IoT) is a transformative technology that connects and empowers a vast network of smart devices, enabling seamless communication and data exchange. And there are different types of IoT Architecture, three-layer architecture, SoA-based Architecture, and the Middleware Architecture.

With the integration of identification and tracking technologies like RFID, IoT offers numerous benefits and opportunities across industries. However, there are several challenges that need to be addressed for widespread adoption and effective implementation of IoT. These challenges include cost, power consumption, range limitations, security and privacy concerns, lack of flexibility, and limited data storage and processing capabilities. It is crucial to overcome these challenges to unlock the full potential of IoT in terms of optimizing processes, improving decision-making, and enhancing user experiences. Communication is a vital part of IoT. Various protocols and standards are used to facilitate communication between devices, gateways, and networks.

IoT finds application in several domains. Industries can benefit from IoT through enhanced production processes and worker safety. Smart agriculture leverages IoT to optimize resource usage in farming practices. Smart cities use IoT to manage utilities, transportation, waste management, and more, leading to increased efficiency and improved quality of life for citizens. In healthcare, IoT enables remote monitoring, preventive care, and more efficient allocation of healthcare resources.

In summary, IoT presents immense opportunities for innovation and optimization across industries. Overcoming challenges related to cost, power consumption, security, and flexibility will be pivotal in harnessing the full potential of IoT. By leveraging communication protocols and standards, as well as exploring various applications in different sectors, IoT has the potential to revolutionize the way we live, work, and interact with our environments.

References

[1] "What is the internet of things?," IBM, https://www.ibm.com/topics/internet-of-things (accessed Oct. 16, 2023).

[2] Ashton, K. That 'Internet of Things' thing. RFID J. 2009, 22, 97–114.

[3] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," Information, vol. 12, no. 2, p. 87, 2021. doi:10.3390/info12020087

[4] S. Li, L. D. Xu, and S. Zhao, "The internet of things: A survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2014. doi:10.1007/s10796-014-9492-7

[5] J.-S. Ulmer, J.-P. Belaud, and J.-M. Le Lann, "A pivotal-based approach for enterprise business process and is integration," Enterprise Information Systems, vol. 7, no. 1, pp. 61–78, 2013. doi:10.1080/17517575.2012.700326

[6] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the Internet of Things: State of the Art," Robots and Sensor Clouds, pp. 55–75, 2015. doi:10.1007/978-3-319-22168-7_3

[7] A. Taivalsaari and T. Mikkonen, "A taxonomy of IOT client architectures," IEEE Software, vol. 35, no. 3, pp. 83–88, 2018. doi:10.1109/ms.2018.2141019

[8] F. Mattern and C. Floerkemeier, "From the internet of computers to the internet of things," *Lecture Notes in Computer Science*, pp. 242–259, 2010. doi:10.1007/978-3-642-17226-7_15

[9] A. Čolaković and M. Hadžialić, "Internet of things (IOT): A review of Enabling Technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018. doi:10.1016/j.comnet.2018.07.017

[10] A. P. Ciganek, W. (Dave) Haseman, and K. Ramamurthy, "Time to decision: The drivers of innovation adoption decisions," *Enterprise Information Systems*, vol. 8, no. 2, pp. 279–308, 2012. doi:10.1080/17517575.2012.690453

[11] H. Panetto and J. Cecil, "Information Systems for Enterprise Integration, interoperability and networking: Theory and applications," *Enterprise Information Systems*, vol. 7, no. 1, pp. 1–6, 2013. doi:10.1080/17517575.2012.684802

[12] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in 2012 2nd International Conference on Consumer Electronics, Communications and Networks, 2012, pp. 537–1285, doi: 10.1109/CECNet.2012.6201508.

[13] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks," Sensors., vol. 20, no. 9, 2020, doi: 10.3390/s20092495.

[14] Q. Chi, H. Yan, C. Zhang, Z. Pang, and D. X. Li, "A reconfigurable smart sensor interface for industrial WSN in IOT environment," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1417–1425, 2014. doi:10.1109/tii.2014.2306798

[15] S. Karthikeyan, G. J. Rani, K. Ramamoorthy, T. Chelladurai, and Dr. E. Thangaselvi, "The Industrial Internet of Things (IIoT): An Analysis Framework for Industry 4.0 Applications," INTERNATIONAL CONFERENCE ON RESEARCH IN SCIENCES, ENGINEERING; TECHNOLOGY, 2022. doi:10.1063/5.0081996

[16] B. B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of internet of things in Smart Agriculture: A Survey," Future Generation Computer Systems, vol. 126, pp. 169–184, 2022. doi:10.1016/j.future.2021.08.006