A Roadmap for IoT Network Research and Development

Ziyad almudayni[1†], Ben Soh[2††], Alice Li[3††]

Department of Computer Science and Information Technology, La Trobe University, Melbourne, Australia

Abstract
To make the research and development in IoT networks witness a significant improvement and last for a long period, it is always important to attract new researchers to work on this area and be a part of it. The best way to attract researchers to work in any research area and have their interest is to give them a clear background and roadmap about it. In this way, researchers can easily find a deep point to start their research based on their interest. This paper presents an overview and roadmap about IoT technologies from the most five vital aspects: IoT architecture, communication technologies, type of IoT applications, IoT applications protocols and IoT challenges.

Key words:
Maintenance, Security, Scalability, CoAP and MQTT.

1. Introduction

The Internet of things (IoT), in simple terms, is a machine-to-machine communication via the Internet used to perform specific tasks. Humans also can act as a third party in connecting and communicating with machines via controllers such as smartphones [1]. IoT technologies have played a vital role in simplifying work through saving time and effort [2]. Therefore, this technology might witness an extraordinary rise in the coming years, and the number of connected devices in use globally might reach over 100 billion. For this reason, researchers have been working to develop this technology from many aspects such as security, data rate, coverage and more to make it a more reliable and scalable technology. In order to make the research and development in IoT networks witness a significant improvement and last for a long period, it is always important to attract new researchers to work on this area and be a part of it. The best way to attract researchers to work in any research area and have their interest is to give them a clear background and roadmap about it; in this way, researchers can easily find a deep point to start their research based on their interest. This paper presents an overview and roadmap about IoT technologies from the most five vital aspects. Based on these aspects, a researcher might be able to create a clear plan to start their research. The first aspect is the fundamental of the IoT structure and its layers. The second aspect is related to the communication technologies that link IoT devices in a network. The third aspect is about selecting an environment area for deploying IoT devices to provide services to end-users, based on the IoT application types. The fourth aspect is related to the communication protocols at the application layer. The final aspect concerns the challenges that IoT systems face.

2. Background and Roadmap for IoT (IoT Architecture)

The IoT architecture can be categorised into four main layers: perception layer, network layer, middleware layer and application layer as shown in Fig. 1.[3]. The main objective of this classification is to assist IoT developers in identifying the area of any technical issues based on this classification.

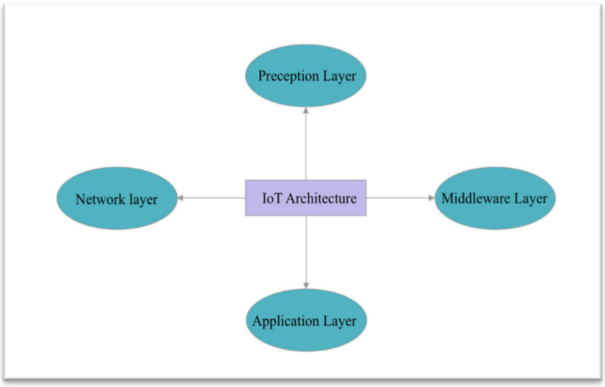

Fig. 1 IOT ARCHITECTURE.

2.1 The Perception Layer

The perception layer is the first layer that the IoT system begins to execute. It is likely same as the physical layer in the OSI network. This layer is responsible for collecting and exchanging data from the surrounding areas in the physical world [4]. Sensors and actuators are the two primary items that can detect and sense the changes in the real-world environment, for example measuring the temperature of a room and then sending the collected data to the next layer, which is the network layer for connectivity [5].

Sensors: A sensor is an electronic device that can detect and sense the physical environment such as measuring the temperature by using a thermistor [6].

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.7

Actuators: An actuator is a machine that can move the IoT devices from one state to another state such as switching the light off or on by using a Rely device [7].

IoT Data: The IoT objects such as sensors and actuators generate two types of data. Measurement data is when sensors generate data to detect and sense the events in real world of the surrounding environment such as temperature, humidity etc. Context-data provides information about the description of an object and its condition such as battery-life, latency, etc. and sends this information to the users [8].

IEEE 802.15.4 was introduced in 2003 as a wireless personal area network standard for the physical layer and MAC, which is preferable in cases where high power and high-rate wireless communication systems are not required [9]. It covers small areas only, and the maximum transmission range that it can reach is about 100m [10].

2.2 The Network Layer

The network layer is the second layer in the IoT architecture. It acts as the brain of the IoT systems [11]. The primary aim of the network layer is to gather data from the perception layer and transmit this information to the middleware layer for further analysis and processing. Internet getaways such as WiFi, RFID, etc. operate at this layer to execute different network communication services [12]. In this section, the communication technologies, routing, and the architecture of IoT networks will be discussed.

Communication technologies can be defined as the mechanism type that links IoT devices in a network for the purpose of data transmission. There are various communication mechanisms in the market, such as WiFi. In this section, seven communication mechanisms with their description are listed below. There are more than these seven in the market; however, we believe the following seven are the most important once as shown in Fig. 2.

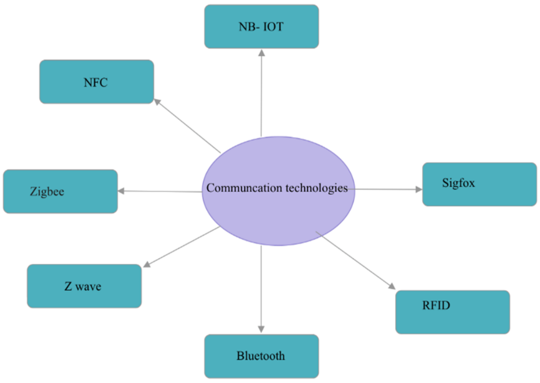

Fig. 2 Communication technologies.

Sigfox: Sigfox could be considered as the first global IoT network in which IoT devices can transmit data without the need to install any network connections. The management of transmitting data between IoT devices proceeds in the cloud by the software-based communication that the Sigfox offers. This management leads to minimising the cost of connectivity and power consumption [13]. The Sigfox network architecture consists of three majors' parts: base stations, IoT devices and central networks. The communication protocol in Sigfox is designed to send small messages (0 to 12 bytes) [14].

NB-IOT: Researchers are giving more concern to the NB-IoT due to its low-cost, low power consumption, long-distance indoor coverage. It is the most popular choice for most of the IoT nodes [15]. The bandwidth of NB-IoT for both uploading and downloading is the best choice for low-cost devices, and it is about 180 kHz, which is considered as a low-frequency bandwidth. NB-IoT provides connectivity for IoT devices over long-distances, and the maximum coverage that it can serve is about 15km. The latency in NB-IoT is preferable in many IoT applications, which is about 10ms [16].

Zigbee: Zigbee has been launched as a wireless communication protocol. In comparison with other communication protocols, the cost of establishing a ZigBee network is low. It covers small areas with a low data rate and can provide service monitoring in small areas, such as homes [17]. The coverage of a Zigbee network is the same as a Wi-Fi network because both provide the same bandwidth, which is 2.4 GHz [18].

NFC: Near Field Communication was introduced as wireless communication technology to provide connectivity in a very small area. NFC has added value and brings many advantages to the IoT technology. One of its remarkable gains is in the way of communications, since it does not require any pairing to set up, so it is much easier than Bluetooth, which requires paring [19]. The main disadvantage of NFC is the short coverage, which is about 4 cm [20].

Radio Frequency Identification: RFID can be classified as one of the wireless communication technologies. The primary objective of RFID is to collect data from the surrounding areas in a limited range from 1m to 12m by broadcasting radio signals and it processes this information to implement services such as monitoring, tracking, etc. [21]. RFID tags and RFID readers are the two main parts of the RFID system; tags such as cards collect information by broadcasting radio waves, whereas readers act as a brain to execute processing [22].

Bluetooth: Bluetooth technology can be utilised to provide connectivity for IoT devices in a limited range. The maximum range that Bluetooth can cover is about 10m. Bluetooth operates with low power, and there is a limit in the number of devices that can connect at the same time, which is about 8 devices. It is suitable for small areas such as homes and apartments [23].

Z-Wave: Z-Wave was introduced to provide connectivity for many IoT applications in small zones such as homes. It has a low power consumption MAC standard. The maximum coverage that the Z-Wave can reach is about 30 metres. It is suitable for small messages, and it provides P2P communication. Master/slave is the architecture that the Z-Wave follows [24].

The power consumption of the wireless techniques for the IoT devices communication differs from protocol to another protocol, and each protocol has its own specifications other than the power consumption such as distance and data rare and more specifications.

Table 1: State of the art comparison

	Proximity	***NFC***	***Zigbee***	***BT***	***WIFI***	***LORA***
Distance	1 mm	10 cm	10-100 mm	10-100 mm	30-50 m	~km
Data rate	8-32 Gbps	0.021-0.48 Mbps	0.02-0.2 Mbps	0.8-2.1 Mbps	300 Mbps (11g) 7 Gbps (11ac,11d)	200 Kbps
Energy-efficiency	4 pJ/b	1-50 nJ/b	5 nJ/b	15 nJ/b	5 nJ/b	1 uJ/b
Security	High	Medi	Low	Low	Medi or high	Unknown

Based on these specifications, the IoT systems developers can select a suitable communication protocol to fit in the environment they are designing. In Table 1. In [25], the authors collected information about five wireless techniques, namely Proximity, NFC, ZigBee, Wi-Fi and LoRa to compare them in terms of distance, data rate, energy efficiency and security.

Network Architecture

The topologies of IoT networks are divided into two main categories: centralized and distributed IoT networks. The IoT system developers design the network topology of their systems based on the IoT applications' requirements. In this section, centralized and IoT networks will be discussed.

a) Centralized IoT Networks

In centralized networks, all IoT devices process, control, and store data in one single gateway. The network's workload will not be distributed into several gateways to balance the traffic in the network. As all nodes share the same gateway, more congestion and traffic are expected. The main disadvantage of this type of network is when the central gateway shuts down; all IoT nodes will be disconnected [26].

b) *Distributed IoT Networks*

In distributed IoT networks, the processing, controlling and storing of data in IoT devices are distributed in several gateways, and each gateway works independently to balance the workload of IoT nodes. This network brings many advantages to the IoT systems in term of many aspects, such as low latency, high flexibility and high scalability. Due to these features, the distributed IoT network is much better than the centralized once [27].

Routing in IoT

Routing can add value to IoT technology in general and can play an essential role in developing the IoT-network environment. Routing protocols can discover the optimal paths between any two nodes among multiple paths for packets to be delivered to its destination [28]. Routing algorithms are responsible for deciding the optimal route between the sender and the receiver. Researchers and developers aim to suggest and develop different routing algorithms to achieve several goals such as increasing the network lifetime and minimizing the latency and more [29].

2.3 The Middleware Layer

The middleware layer is the third layer in the IoT architecture. It analyzes and stores the received data from the network layer [30]. It works as a bridge to link the IoT system to the computing systems and databases for further processing. It is responsible for preparing the data to be utilized in the application layer. Machine learning and artificial intelligence systems might be used at this layer to transform the collected data into valuable information to support the system in the decision-making process at the application layer [31].

2.4 The Application Layer

The application layer is the top layer in the IoT architecture and its main purpose to provide services for the end-users [32]. This layer generates the processed data from the middleware layer to meet the QoS in IoT applications in various cases to deliver services to the end-user. It works as a chain to enable end-users to use IoT applications such as smart homes, smart cities, smart industries, etc. End-user can access these IoT applications through internet-enabled devices such as smartphone, laptop, television, etc. [33]. In this section, the most popular IoT applications and their messaging protocols will be defined.

a) IoT application types

In this section, application types refer to the name of applications when delivering services for end-users. Therefore, applications vary from one to another based on the environment and the delivered services to the end-user. In this section, the most important seven IoT applications are listed as shown in Fig .3.

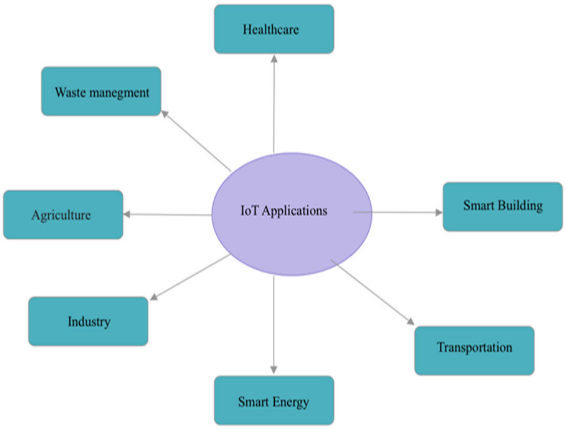

Fig. 3 Application types for users.

IoT in healthcare: The main objective of proposing IoT is to provide more convenient life for humans by organizing their basic tasks. The treatment of patients in the healthcare systems can be enhanced when the IoT devices utilized in the system [34]. This can be achieved by combining the IoT sensors with the health monitoring gadgets used by patients to provide further analyses. These sensors gather information about the status of patients and send this information to the internet for further processing. Doctors and nurses use the analysed and processed data to monitor the status of patients remotely [35]. Moreover, healthcare systems might witness significant improvements when applying IoT systems in the environment regarding data accuracy when reporting the patient's status like their temperature and blood pressure to doctors and nurses compared to writing the data manually where mistakes might happen.

IoT in smart buildings: The smart building has been established to provide more convenient living arrangements for residents. The IoT systems can monitor and control the appliances in building like remote monitoring via Internet [36]. Switching appliances off and on remotely through smartphone apps can play an important role in reducing the power consumption as the control of these appliances can be done easily. IoT systems can also provide safety monitoring to protect residents from any external risks by using cameras and alarm systems effectively [37]. In addition, smart buildings might play an important role not directly in decreasing the conflicts between the family members because everything in the house can be handled easily. For instance, an intelligent vacuum can clean the living room automatically, which will allow the family members to have more time to set together in a clean place without making any effort.

IoT in transportation: Nowadays, the demand for the public transportation system (PTS) has risen recently due to the significant increase in the number of daily trips because of growing urbanization. The demand for PTS in urban cities is high, and the traditional PTS has achieved significant contributions in terms of reducing air pollution, traffic accidents and road congestion [38]. One of the main disadvantages of using public transportation is the time that passengers spend in stations waiting for buses and trains. Knowing the location of buses and the exact arrival time will encourage commuters to use public transportation in their daily life, and this can be achieved by integrating the IoT systems into PTS [39]. From an economic perspective, the income of public transportation might increase when integrating IoT systems in their environment because the number of passengers will increase when the trips are scheduled accurately.

IoT in smart energy: The IoT sensors can be integrated with electronic gadgets to measure and analyse the power consumption of these gadgets for further processing and monitoring [40]. Monitoring power consumption effectively can play an essential role in reducing the cost of bills. It also benefits to the environment in several ways such as minimizing the air pollution. Electric companies will also benefit, as this monitoring will decrease the pressure and load on these companies in terms of reading and reporting consumers' bills [41]. All that will lead to increase the confidence between the electric companies

IoT in agriculture: Establishing the IoT technology in the agriculture environment can play an essential role in improving the farming environment. Farmers can easily monitor their crop yield when effectively using IoT devices [42]. This technology will bring several benefits to the agriculture environment in term of many aspects. It helps farmers to limit the time to produce more with less effort. The performance of the production can be examined after generating the data from the IoT sensors [43]. The IoT sensors will assist in increasing the success of crop production as these sensors can make destinations in early stages; for instance, greenhouse agriculture can be closed directly when sensors detect heavy rain.

IoT in industry: IoT systems in industry can handle and control the manufacturing processes at the real-time without any delays. The M2M communications can play an essential role in reducing the number of workers in industries, which minimize the cost of manufacturing. Integrating IoT systems into various industries has enhanced efficiency, improved the QoS as well as maintenance services. Supervisors in industries can easily examine the performance of manufacturing by pulling the data from the IoT sensors [44]. From an economic perspective, the number of industries in the country might increase as traders can establish new industries with less cost compared to the past, as the number of workers will decrease when integrating IoT systems into their environment.

IoT in smart waste management: Waste management is one of the most common concerns in modern urban regions that experts and developers are trying to overcome. The cost of collecting containers and the space to store wastes are the two main reasons that make waste management more complicated. IoT technology can play an essential role in enhancing the waste management systems [45]. Sensors and actuators can be installed in containers to determine the load level of containers to help collectors to distinguish between full and empty containers more easily, so that they may better define their routes. This approach will result in minimizing the cost of managing waste collection and enhance the quality of service in recycling [46].

b) *IoT application protocols*

This section examines the IoT protocols concerning the mechanism that mechanism that facilitates communication between machine and machine at the application layer. There are many application protocols; however, this section only lists the five most vital protocols as shown in Fig .4

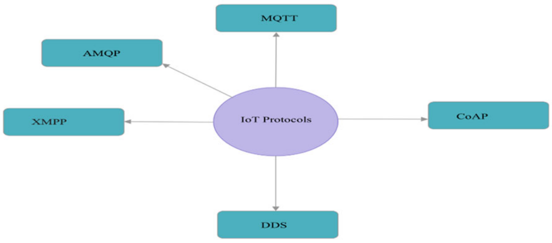

Fig. 4 Application protocols.

Message queue telemetry transport (MQTT): In 1999, the MQTT messaging protocol was introduced, and it is considered one of the earliest machine-to-machine communication protocols [47]. MQTT follows a publish/subscribe model that operates over TCP connections, and it uses a broker to link publishers to subscribers. The structure of MQTT allows it to operate in poor networking conditions and with resource restrictions. In comparison to other messaging protocols, MQTT is one of the most preferred options for IoT applications due to its simplicity and the small size of the header [48].

Constrained Application Protocol (CoAP): The communication protocols in IoT are distinguished from one another depending on which layer the transmissions of data occurs. CoAP can be broadly defined as a standard web transfer protocol in which the data are transmitted at the application layer [49]. The UDP is the communication protocol that operates on CoAP. It is a M2M communication protocol mechanism that offers a client/server interaction model among IoT devices [50].

Extensible messaging and presence protocol (XMPP): In 1999, Jeremie Miller introduced the XMPP as a standard protocol to provide communication between machines. XMPP provides an Instant Messaging (IM) service to send and receive messages among users in real-time [51]. In addition to messaging, chat, voice and video calls etc., can be implemented by the XMPP and give these applications security support in terms of access control, authentication and encryption services. As the XML (extensible markup language) is the language used on text messaging, the request/response and publish/subscribe methods can be executed in XMPP [52].

Advanced message queuing protocol (AMQP): In 2003, the AMQP was introduced as a machine-to-machine communication protocol at the application layer over a TCP connection [53]. One of the main purposes of AMQP is to allow various applications and systems to exchange data between different platforms, written in several languages. The publish/subscribe is followed by the old version (AMQP 0.9.1) in which the broker used to exchange data from the publisher to the subscriber. In the newer version of AMQP does not exactly follow the publish/subscribe model and more flexibility can be provided. It also supports different communications mechanisms, such as client-to-client communication [54].

Data distribution service (DDS): The Object Management Group (OMG) launched the DDS as a real-time system protocol that follows the publish/subscribe model to allow machines to send and receive messages. The structure of other publish/subscribe protocols is centralized, whereas the DDS follows the opposite. DDS is based on P2P communication where publishers can directly receive and send messages from and to subscribers directly without knowing the source of data as all descriptions in the packages [55].

3. IoT Challenges

Researchers are continuously working to overcome the challenges faced by IoT technology. In this section, five most vital challenges that IoT systems faces are presented below (see Fig .5).

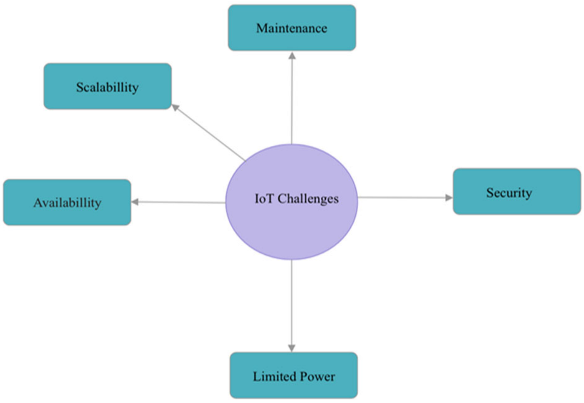

Fig. 5 IoT Challenges.

3.1 Security

Securing IoT systems is one of the most critical challenges that experts and researchers have been trying to overcome. Exchanging data among IoT nodes should be protected from any external attack to create a confidential IoT environment [56]. Protecting IoT devices will encourage consumers to utilise the IoT systems in their homes, since they know their privacy is protected. As far as we know, there are three main research areas in the IoT systems that can be developed to satisfy the QoS in the IoT systems: authentication, authorisation, and privacy. Authentication can be broadly described as the IoT devices' ability to identify one another and define IoT services during communications to protect the systems from attacks from unknown users or services [57]. Authorisation comes after the process of authentication and makes the communication between the IoT devices more secure by giving each device the right to use limit resources [58]. Privacy is the most critical part of IoT security as some applications contain sensitive information such as in healthcare applications, which must be fully secure from any attacks. Protecting data privacy in the IoT devices can be achieved through various techniques such as anomaly detection, cryptographic, and blockchain [59].

3.2 Limited power

Power consumption in IoT systems should be limited because the IoT devices' batteries have energy and cost restrictions [60]. Due to the massive rise in the number of IoT devices, there is now a storage demand to promote IoT networks' energy efficiency. In addition to the number of IoT devices, researchers have proposed several complex algorithms to improve other parameters such as security, data rate and bandwidth, which can contribute to increasing the workload and consuming more power [61]. To the best of our knowledge, researchers have to focus on three network areas to reduce the power consumption in the IoT devices. These areas are the routing and clustering in the WSNs, and the fog computing services in the IoT networks. In addition to the network layer, developers can improve the energy efficiency of the IoT systems through various layers and areas such as the CoAP and MQTT in the application layer. Experts and researchers have achieved significant contributions to enhance the energy efficiency in IoT networks in terms of routing and clustering of WSNs, and most of the challenges have been overcome. On the other hand, there are many scopes than can be achieved in fog computing services to reduce the power consumption, such as developing the scheduling, offloading and balancing the IoT systems' tasks in the fog nodes.

3.3 Availability

As the IoT devices require real-time processing, the devices should be available all the time to avoid delays. In some cases, a service might not be available for a user when he/she sends a request, which might negatively impact the work process, and leading to poor outcomes [62]. Several reasons might affect the IoT systems and make it unavailable and not ready for use. These reasons can be like sensors ageing, dead battery, and more [63]. Researchers have to be aware of the quality and the lifetime of the sensors and hardware devices to make the system available as long as they can.

3.4 Scalability

Scalability is the ability of the IoT systems to handle the growth in the number of IoT devices while overcoming the challenges associated with that growth [64]. Horizontal sensing and vertical sensing are the two main features that have to be enhanced to improve IoT systems' scalability. Adding more devices and nodes to the network belongs to the horizontal sensing, whereas increasing the capacity of a network by adding more resources such as CBU, RAM, and Power belongs to vertical sensing [65]. Achieving a high level of scalability will increase the IoT devices' chance to become successful in the future and to be more reliable. Researchers must focus on finding a way to add more resources, such as CPU and IoT devices without affecting the system's interoperability. A system is called interoperable when multiple IoT sensors can work together in the right place and time to perform functions without any issues [66].

3.5 Maintenance

The cost of maintaining IoT devices might be more expensive than establishing them. It is vital in IoT to have a resiliency system in which nodes can recover and fix errors without any interactions to reduce the cost of maintenance. There are various ways to reduce the cost of maintenance in the IoT environment. The deployment of the IoT devices has to be set in such a way that they can easily be located when they need to be fixed. It is vital to be aware of the IoT devices' range as these devices work with a limited range to avoid damages and incorrect results [67]. The quality of the IoT sensors has to be high to avoid maintains as much as possible.

5. Conclusion and Future Work

Before beginning to research any science area and before going more deeply into it, it is essential to have a complete background and roadmap about the targeted area. This paper aims to attract more new researchers and developers to start their research in IoT networks. This paper has provided researchers with a comprehensive background about the area in terms of five main aspects: IoT architecture, communication technologies, type of IoT applications, IoT applications protocols and IoT challenges. Future studies will investigate and analyse IoT networks' five most vital challenges individually to help researchers determine their paths when targeting a challenge from the five mentioned challenges.

References

[1] F. E. F. Samann, S. R. Zeebaree, and S. Askar, “IoT provisioning QoS based on cloud and fog computing,” Journal of Applied Science and Technology Trends, vol. 2, no. 01, pp. 29–40, 2021.

[2] S. Zafar, G. Miraj, R. Baloch, D. Murtaza, and K. Arshad, “An IoT Based Real-Time Environmental Monitoring System Using Arduino and Cloud Service”, Eng. Technol. Appl. Sci. Res., vol. 8, no. 4, pp. 3238–3242, Aug. 2018.

[3] V. Tiwari, A. Keskar, and N. C. Shivaprakash, “Design of an IoT Enabled Local Network Based Home Monitoring System with a Priority Scheme”, Eng. Technol. Appl. Sci. Res., vol. 7, no. 2, pp. 1464–1472, Apr. 2017.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in Internet-of-Things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[5] A. Rayes and S. Salam, “The things in iot: Sensors and actuators,” in Internet of Things From Hype to Reality, Springer, 2017, pp. 57–77.

[6] C. G. García, D. Meana-Llorián, and J. M. C. Lovelle, “A review about Smart Objects, Sensors, and Actuators.,” International Journal of Interactive Multimedia & Artificial Intelligence, vol. 4, no. 3, 2017.

[7] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, “Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology”, Eng. Technol. Appl. Sci. Res., vol. 10, no. 2, pp. 5441–5447, Apr. 2020.

[8] S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, “Searching for the IoT resources: fundamentals, requirements, comprehensive review, and future directions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2101–2132, 2018.

[9] A. Reziouk, E. Laurent, and J.-C. Demay, “Practical security overview of IEEE 802.15. 4,” in 2016 International Conference on Engineering & MIS (ICEMIS), 2016, pp. 1–9.

[10] A. Gezer and S. Okdem, “☆ Improving IEEE 802.15. 4 channel access performance for IoT and WSN devices,” Computers & Electrical Engineering, vol. 87, p. 106745, 2020.

[11] 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 (CECNet), 2012, pp. 1282–1285.

[12] K. Ozera, K. Bylykbashi, Y. Liu, and L. Barolli, “A fuzzy-based approach for cluster management in VANETs: Performance evaluation for two fuzzy-based systems,” Internet of Things, vol. 3, pp. 120–133, 2018.

[13] W. Ayoub, A. Ellatif Samhat, M. Mroue, H. Joumaa, F. Nouvel, and J.-C. Prévotet, “Technology selection for iot-based smart transportation systems,” in Vehicular ad-hoc networks for smart cities, Springer, 2020, pp. 19–29.

[14] Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovács, I.Z., Mogensen, P., and Sorensen, M.: ‘Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot’, in Editor (Ed.)^(Eds.): ‘Book Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot’ (IEEE, 2017, edn.), pp. 1-5.

[15] K. O. Adefemi Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, “A survey on the security of low power wide area networks: Threats, challenges, and potential solutions,” Sensors, vol. 20, no. 20, p. 5800, 2020.

[16] R. S. Sinha, Y. Wei, and S.-H. Hwang, “A survey on LPWA technology: LoRa and NB-IoT,” Ict Express, vol. 3, no. 1, pp. 14–21, 2017.

[17] Y. Yang, X. Luo, X. Chu, and M.-T. Zhou, Fog-enabled intelligent IoT systems. Springer, 2020.

[18] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of Things (IoT) communication protocols,” in 2017 8th International conference on information technology (ICIT), 2017, pp. 685–690.

[19] D. Serfass and K. Yoshigoe, “Wireless sensor networks using android virtual devices and near field communication peer-to-peer emulation,” in 2012 Proceedings of IEEE Southeastcon, 2012, pp. 1–6.

[20] J. Su, Z. Sheng, A. X. Liu, Z. Fu, and Y. Chen, “A time and energy saving-based frame adjustment strategy (TES-FAS) tag identification algorithm for UHF RFID systems,” IEEE Transactions on Wireless Communications, vol. 19, no. 5, pp. 2974–2986, 2020.

[21] S. F. Khan, “Health care monitoring system in Internet of Things (IoT) by using RFID,” in 2017 6th International Conference on Industrial Technology and Management (ICITM), 2017, pp. 198–204.

[22] M. Collotta, G. Pau, T. Talty, and O. K. Tonguz, “Bluetooth 5: A concrete step forward toward the IoT,” IEEE Communications Magazine, vol. 56, no. 7, pp. 125–131, 2018.

[23] S. Sharma and S. Kumar, “A Review on IoT: Protocols, Architecture, Technologies, Application and Research Challenges,” in 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020, pp. 559–564.

[24] T. Salman and R. Jain, “A survey of protocols and standards for internet of things,” arXiv preprint arXiv:1903.11549, 2019.

[25] Sen, S., Koo, J., and Bagchi, S.: ‘TRIFECTA: security, energy efficiency, and communication capacity comparison for wireless IoT devices’, IEEE Internet Computing, 2018, 22, (1), pp. 74-81

[26] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, “Artificial intelligence enabled Internet of Things: Network architecture and spectrum access,” IEEE Computational Intelligence Magazine, vol. 15, no. 1, pp. 44–51, 2020.

[27] D. Arellanes and K.-K. Lau, “Evaluating IoT service composition mechanisms for the scalability of IoT systems,” Future Generation Computer Systems, vol. 108, pp. 827–848, 2020.

[28] S. Chen, S. Wang, and J. Huang, “Analysis of Best Network Routing Structure for IoT,” in International Conference on Wireless Algorithms, Systems, and Applications, 2019, pp. 556–563.

[29] A. J. Dey and H. K. D. Sarma, “Routing Techniques in Internet of Things: A Review,” Trends in Communication, Cloud, and Big Data, pp. 41–50, 2020.

[30] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, “Internet of Things (IoT): A vision, architectural elements, and security issues,” in 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017, pp. 492–496.

[31] S. Bansal and D. Kumar, “IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication,” International Journal of Wireless Information Networks, pp. 1–25, 2020.

[32] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, “Study and application on the architecture and key technologies for IOT,” in 2011 International Conference on Multimedia Technology, 2011,

[33] A. Abdullah, H. Kaur, and R. Biswas, “Universal Layers of IoT Architecture and Its Security Analysis,” in New Paradigm in Decision Science and Management, Springer, 2020, pp. 293–302.pp. 747–751.

[34] M. H. Alanazi and B. Soh, “Behavioral Intention to Use IoT Technology in Healthcare Settings”, Eng. Technol. Appl. Sci. Res., vol. 9, no. 5, pp. 4769–4774, Oct. 2019.

[35] K. R. Darshan and K. R. Anandakumar, “A comprehensive review on usage of Internet of Things (IoT) in healthcare system,” in 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), 2015, pp. 132–136.Eng. Technol. Appl. Sci. Res., vol. 9, no. 5, pp. 4769–4774, Oct. 2019

[36] T. Malche and P. Maheshwary, "Internet of Things (IoT) for building smart home system," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017, pp. 65–70.

[37] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," International journal of engineering science and computing, vol. 6, no. 5, 2016.

[38] A. Ladha, P. Bhattacharya, N. Chaubey, and U. Bodkhe, "IIGPTS: IoT-based framework for intelligent green public transportation system," in Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), 2020, pp. 183–195.

[39] B. K. Harini, A. Parkavi, M. Supriya, B. C. Kruthika, and K. M. Navya, "Increasing efficient usage of real-time public transportation using IOT, cloud and customized mobile app," SN Computer Science, vol. 1, pp. 1–8, 2020.

[40] B. K. Barman, S. N. Yadav, S. Kumar, and S. Gope, "IOT based smart energy meter for efficient energy utilization in smart grid," in 2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE), 2018, pp. 1–5.

[41] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 847–870, 2018.

[42] J. Muangprathub, N. Boonnam, S. Kajornkasirat, N. Lekbangpong, A. Wanichsombat, and P. Nillaor, "IoT and agriculture data analysis for smart farm," Computers and electronics in agriculture, vol. 156, pp. 467–474, 2019.

[43] B. Ragavi, L. Pavithra, P. Sandhiyadevi, G. K. Mohanapriya, and S. Harikirubha, "Smart Agriculture with AI Sensor by Using Agrobot," in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 1–4.

[44] S. Aheleroff et al., "IoT-enabled smart appliances under industry 4.0: A case study," Advanced engineering informatics, vol. 43, p. 101043, 2020.

[45] K. D. Kang, H. Kang, I. Ilankoon, and C. Y. Chong, "Electronic waste collection systems using Internet of Things (IoT): Household electronic waste management in Malaysia," Journal of cleaner production, vol. 252, p. 119801, 2020.

[46] G. K. Shyam, S. S. Manvi, and P. Bharti, "Smart waste management using Internet-of-Things (IoT)," in 2017 2nd international conference on computing and communications technologies (ICCCT), 2017, pp. 199–203.

[47] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and open issues of MQTT protocol," in 2017 international conference on engineering & MIS (ICEMIS), 2017, pp. 1–6.

[48] D. Glaroudis, A. Iossifides, and P. Chatzimisios, "Survey, comparison and research challenges of IoT application protocols for smart farming," Computer Networks, vol. 168, p. 107037, 2020.

[49] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP," in Digital Twin Technologies and Smart Cities, Springer, 2020, pp. 151–175.

[50] P. Bellavista and A. Zanni, "Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP," in 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), 2016, pp. 1–6.

[51] P. Saint-Andre, "XMPP: lessons learned from ten years of XML messaging," IEEE Communications Magazine, vol. 47, no. 4, pp. 92–96, 2009.

[52] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A. Spirito, "The virtus middleware: An xmpp based architecture for secure iot communications," in 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–6.

[53] J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, and P. Manzoni, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), 2015, pp. 931–936.

[54] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," ACM Computing Surveys (CSUR), vol. 51, no. 6, pp. 1–29, 2019.

[55] S. Profanter, A. Tekat, K. Dorofeev, M. Rickert, and A. Knoll, "OPC UA versus ROS, DDS, and MQTT: performance evaluation of industry 4.0 protocols," in 2019 IEEE International Conference on Industrial Technology (ICIT), 2019, pp. 955–962.

[56] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in Digital twin technologies and smart cities, Springer, 2020, pp. 123–149.

[57] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future generation computer systems, vol. 82, pp. 395–411, 2018.

[58] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," IT Professional, vol. 19, no. 5, pp. 27–33, 2017.

[59] T. Qamar, N. Z. Bawany, and N. A. Khan, "EDAMS: Efficient Data Anonymization Model Selector for Privacy-Preserving Data Publishing", Eng. Technol. Appl. Sci. Res., vol. 10, no. 2, pp. 5423–5427, Apr. 2020.

[60] Y. Yang, X. Luo, X. Chu, and M.-T. Zhou, Fog-enabled intelligent IoT systems. Springer, 2020.pr. 2020.

[61] A. Al-Marghilani, "Comprehensive Analysis of IoT Malware Evasion Techniques", Eng. Technol. Appl. Sci. Res., vol. 11, no. 4, pp. 7495–7500, Aug. 2021.

[62] S. Swain and R. Niyogi, "FESC: functionally equivalent service composition," Internet of Things, vol. 9, p. 100151, 2020.

[63] M. Singh, G. Baranwal, and A. K. Tripathi, "QoS-Aware Selection of IoT-Based Service.," Arabian Journal for Science & Engineering (Springer Science & Business Media BV), vol. 45, no. 12, 2020.

[64] A. Gupta, R. Christie, and P. R. Manjula, "Scalability in internet of things: features, techniques and research challenges," Int. J. Comput. Intell. Res, vol. 13, no. 7, pp. 1617–1627, 2017.

[65] T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, "Enabling distributed intelligence for the Internet of Things with IOTA and mobile agents," Computing, vol. 102, no. 6, pp. 1345–1363, 2020.

[66] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," Mobile Networks and Applications, vol. 24, no. 3, pp. 796–809, 2019.

[67] F. Civerchia, S. Bocchino, C. Salvadori, E. Rossi, L. Maggiani, and M. Petracca, "Industrial Internet of Things monitoring solution for advanced predictive maintenance applications," Journal of Industrial Information Integration, vol. 7, pp. 4–12, 2017.