DOI: https://doi.org/10.17762/turcomat.v11i3.13604

Research Article

Internet of Things (IoT) Networks: Architecture, Applications, and Future Directions

Amit Kumar Mishra

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract: The Internet of Things (IoT) networks, including their design, applications, future directions, difficulties, and constraints, are thoroughly discussed in this research study. The explanation of IoT networks' design, covering definitions and components, as well as centralized and decentralized networks, follows an overview of IoT networks' significance. The applications of IoT networks are examined in the next part, along with specific use examples from the fields of healthcare, manufacturing, transportation, and smart cities. The following section of the article examines new developments in IoT networks, including edge computing, 5G networks, AI, and blockchain technology. The difficulties and constraints of IoT networks, such as security and privacy issues, interoperability and compatibility problems, scalability, and network congestion, are also examined. The final section of the study summarizes the main ideas and research conclusions, highlighting the significance of IoT networks in our increasingly linked society.

Keywords: Security, privacy, interoperability, compatibility, scalability, network congestion, edge computing, 5G networks.

I. Introduction

"Things" that are part of the "Internet of Things" (IoT) are equipped with sensors, software, and network connectivity, giving them the ability to gather and share data with one another and with other devices. The ongoing digital transformation is taking place in many different domains, including medical, industry, transportation, and urban planning[1]. Connected devices and their networks are important to this transformation. This response will concentrate on the architecture, applications, and future directions of potential development of IoT networks.The term "Internet of Things" (IoT) describes a network of actual physical objects that are linked to the internet and are capable of exchanging data and information with one another. These items, often known as "smart devices," have sensors, software, and network connectivity that enable data collection and transmission[2]. Healthcare, industry, transportation, and smart cities are just a few of the sectors being transformed by IoT networks.IoT networks are becoming more and more significant as businesses all over the world continue to utilize this technology to increase operational effectiveness, cut costs, and improve customer experience[3]. Over the coming years, the global IoT industry is anticipated to expand rapidly, increasing in size to an estimated $1.5 trillion by 2030.This study paper's main goal is to give a thorough review of IoT networks, covering its design, uses, and prospects. Also, this study will emphasize the drawbacks and restrictions of IoT networks as well as how they may affect future studies. The reader will have a better knowledge of the potential of IoT network.

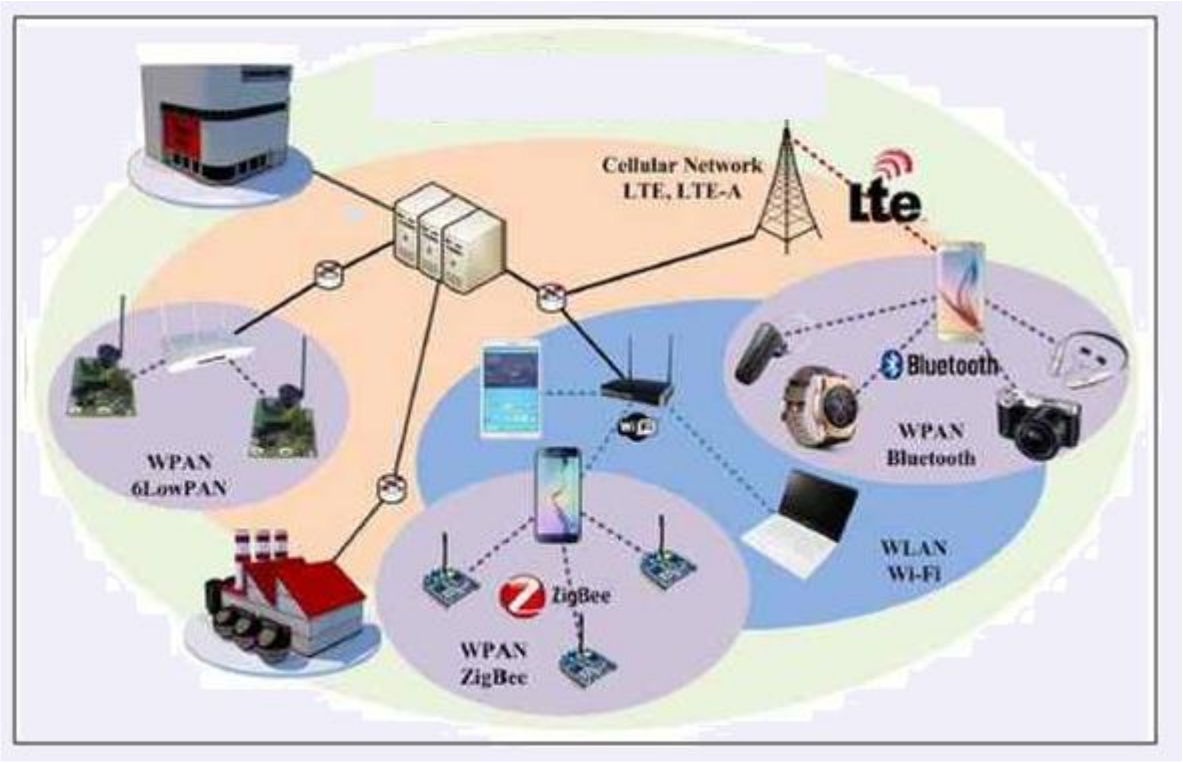

Figure.1 IoT Network

II. Review of Literature

The Internet of Things (IoT) , is an enabling technologies, and potential uses. The authors highlight the obstacles and prospects in this field while discussing the many components of the IoT, such as sensors, communication networks, and data processing systems.The benefits and drawbacks of the IoT are explored in this study, along with concerns about privacy, security, and standardization. The authors in [4], present an overview of the several IoT technologies and talk about why it's important for them to work together.The vision, architectural aspects, and future directions of the IoT are all discussed in this article. The authors in [5]present an overview of the supporting technologies, including sensors, wireless networks, and cloud computing, and examine the different IoT applications, such as healthcare, smart homes, and transportation.This study examines all aspects of the IoT, from its definition and structure to its potential uses. The writers highlight the challenges and potential in the field of IoT and cover its many subjects and developments, such as data analytics, security, and standards.The authors in [6], we'll look at the parallels and differences between WSNs and the Internet of Things. The authors give a rundown of the technologies—sensors, wireless networks, and data processing systems—that make WSNs and the Internet of Things possible, and then describe their many uses in fields like medicine, smart homes, and agriculture.The authors in [7], we'll look at how effective resource management is essential to the growth of cloud-based vehicle networks. The authors offer a resource management paradigm for vehicular networks in the cloud and then analyze the many issues and potential solutions that arise in this setting.The authors in [8]Big data analytics and the Internet of Things are discussed in this article and how they can be used to build smart and connected neighborhoods. The authors in [9]provide an in-depth analysis of the potential and threats associated with the Internet of Things (IoT) in smart cities.

Reference	Year	Focus	Methodology	Key Findings
[8]	2019	General overview	Literature review	Highlights the architecture, applications, and security concerns of IoT.
[9]	2018	Healthcare applications	Literature review	Shows the potential benefits of IoT in healthcare, including remote monitoring and improved patient

				outcomes.
[10]	2019	Manufacturing applications	Literature review	Discusses the various applications of IoT in manufacturing, including predictive maintenance and supply chain optimization.
[11]	2019	Transportation applications	Literature review	Explores the potential benefits of IoT in transportation, including traffic management and vehicle monitoring.
[12]	2018	Smart city applications	Literature review	Discusses the various applications of IoT in smart cities, including energy management and waste reduction.
[13]	2019	General overview	Literature review	Provides a comprehensive overview of IoT applications, challenges, and future directions.
[14]	2019	IoT security	Literature review	Highlights the key security challenges of IoT and suggests potential solutions.
[15]	2018	General overview	Literature review	Provides an overview of IoT technologies, security, and privacy concerns.
[16]	2018	General overview	Literature review	Discusses the enabling technologies, challenges, and open research issues of IoT.
[17]	2018	General overview	Literature review	Provides a comprehensive overview of IoT architecture, technology, applications, security, and future trends.
[18]	2018	IoT and big data	Literature review	Explores the potential benefits of combining IoT and big data analytics.
[19]	2018	Agriculture applications	Literature review	Discusses the various applications of IoT in agriculture, including crop monitoring and irrigation management.
[20]	2018	Energy management applications	Literature review	Explores the potential benefits of IoT in energy management, including demand response and renewable energy integration.
[21]	2018	Smart grid applications	Literature review	Discusses the various applications of IoT in smart grids, including grid monitoring and fault detection.
[22]	2018	Healthcare applications	Literature review	Explores the potential benefits of combining IoT and cloud computing

Table 1. Comparative Study of Various Techniques used for IoT System

III. Architecture of IoT Networks

IoT networks are made up of a variety of parts that cooperate to make it possible to gather, process, and transmit data. An IoT network's essential elements include:

A. Definition and components of IoT networks

i. **Devices**: These are actual physical things with processors, sensors, and network connectivity. Smart household appliances, wearable fitness trackers, commercial machinery, and environmental sensors are a few examples of IoT gadgets.

ii. **Sensors:** Sensors are used to collect data from the physical environment, such as temperature, humidity, pressure, or position. A wide range of sensors, such as accelerometers, gyroscopes, microphones, and cameras, can be used by IoT networks.

iii. **Actuators:** These parts are used to change the environment in response to information gathered by sensors. For instance, an IoT network may employ actuators to modify a room's temperature or turn on and off lighting.

iv. **Network Connectivity:** IoT devices need to be connected to a network to transmit data. Many network technologies, such as Wi-Fi, cellular networks, and Bluetooth, can be used to do this.

v. **Data processing** is necessary in order to make use of the data that IoT devices collect. This can be done on the device itself, on a nearby edge device, or on the cloud. Data analysis, aggregation, and filtering are all examples of processing.

vi. **Storage:**IoT networks may store, process, and analyse data using cloud services. These can include services for data storage, data analytics, and machine learning.

vii. **Applications:** Software applications can be used by IoT networks to let users interact with and manage the network. These can include mobile or web tools that let consumers access and keep tabs on data coming from their Internet of Things (IoT) devices.

viii. **Security:** IoT networks need to be secure to avoid unauthorized access or modification of data. These may include threat detection technologies, access controls, and encryption.

These components work together to enable IoT networks to collect, process, and send data from the real world. IoT networks can offer a number of advantages by fusing these elements, including increased operational effectiveness, lower costs, and better user experiences.

B. Four layers of IoT network architecture

IoT networks can be further divided into blocks or modules, each of which serves a particular function. Depending on the particular use case of the IoT network, these blocks can be organized in a variety of ways. Some of the typical building blocks or modules for IoT network topologies include the following:All physical components of the IoT network, such as sensors, actuators, and gateways, are included in the device layer. These gadgets gather information and talk to other gadgets in the network.All network elements that permit communication between devices, such as Wi-Fi routers, gateways, and switches, are included in the network layer. The network layer also comprises protocols and technologies, such Bluetooth, Zigbee, and LoRa, that allow devices to connect with one another.

i. **Cloud Layer:** This layer consists of cloud-based services that give the IoT network access to storage, compute, and analytics. These services can be used to store data, handle data processing and analysis, and give end users insights.

ii. **Application Layer:** This layer consists of computer programs that give end users access to the information gathered by the Internet of Things network. These programs can be used to display data, start processes, and provide notifications.

iii. **Security Layer:**The security procedures in this layer assure the availability, confidentiality, and integrity of the data gathered by the IoT network. Threat detection, access limits, and encryption are examples of security measures.

iv. **Device Layer:**Device management, network monitoring, and firmware updates are just a few of the tools and services that help network administrators manage the IoT network.

IoT networks can be designed in a variety of ways depending on the network's needs and the individual use case. IoT networks often depend on a combination of physical objects, network elements, cloud-based services, software applications, security methods, and management tools to operate, regardless of the architecture.

C. Centralized and decentralized networks

i. **Centralized Networks**: All data gathered by IoT devices is transmitted to a central server for processing and storage in a centralized IoT network design. On-site or in the cloud are both viable locations for this server. The server is responsible for processing and analyzing data, and may also serve as a gateway to other systems. As all the data is in one place, centralized networks can be simpler to manage and maintain. Yet, centralized networks may be less scalable and more subject to single points of failure.

ii. **Decentralized Networks:** With a decentralized IoT network architecture, data processing and storage is distributed among different devices and systems. For instance, instead of being routed to a centralized server, data gathered by IoT devices may be processed and analyzed on the edge, in a nearby gateway or device. While there are several nodes that can handle data processing and storage, decentralized networks can be more scalable and resilient than centralized networks. Decentralized networks, on the other hand, can be trickier to run and maintain because data is dispersed throughout numerous hardware and software platforms.

Network topologies that are centralized or decentralized each have benefits and drawbacks of their own. The network's size, the amount of data being collected, whether real-time processing is needed, and the required level of security all play a role in the architecture choice. To attain the appropriate level of scalability, robustness, and security, certain IoT networks may employ a hybrid architecture, which mixes centralized and decentralized features.

IV. Applications of IoT Networks

IoT networks are used in a wide range of fields and businesses, including manufacturing, transportation, healthcare, and smart cities. Below is a summary of some of the major IoT network-using industries:

i. Healthcare: By enabling remote patient monitoring, streamlining hospital operations, and giving real-time patient data, IoT networks can improve patient outcomes and lower expenses. IoT devices, for instance, can be used to track patients with long-term diseases like diabetes or heart disease and notify medical professionals of any changes in their state.

ii. Manufacturing: By providing real-time monitoring of production processes and equipment, IoT networks can assist increase operational efficiency and decrease downtime. IoT sensors, for instance, can be used to monitor machine performance and anticipate maintenance requirements prior to a breakdown.

iii. Transportation: IoT networks can aid in enhancing user experience, reducing congestion, and improving safety in the transportation sector. IoT sensors, for instance, can be used to track traffic patterns and modify traffic lights to improve flow.

IoT networks have the potential to enhance urban environments' sustainability, safety, and livability. IoT sensors, for instance, can be used to monitor air quality, control energy use, and improve waste management.

A. Examples of specific use cases

The following are some particular use cases for IoT networks:

a) **Smart Homes**: IoT devices can be utilised to build energy-efficient, safe, and simple to maintain smart houses. For instance, IoT-enabled security systems can send out real-time notifications if there is any unexpected activity in the home, while IoT-enabled thermostats can automatically adjust the temperature based on user preferences and occupancy.

b) **Asset tracking**: IoT networks can be used to track assets like inventory, equipment, and vehicles in real time. For example, IoT sensors can be used to monitor the location and condition of products in transit, enabling organizations to optimize their supply chain operations.

c) **Environmental Monitoring:** IoT networks can be used to keep an eye on things like weather patterns, water quality, and air quality. IoT sensors, for instance, can be used to forecast weather patterns or identify pollution levels in streams to assist stop natural disasters.

d) **Agriculture:** Agricultural operations including irrigation, fertilizer, and pest control can be monitored and optimized via IoT networks. IoT sensors, for instance, can be used to enhance crop development and output by monitoring soil moisture levels and adjusting irrigation systems.

V. IV. Future Directions of IoT Networks

A. Emerging trends in IoT networks

Digital twins are virtual reproductions of actual systems or gadgets. They can be used to imitate the behavior of systems in the real world because they are developed using sensor data. Design, testing, and maintenance of IoT systems and devices can be made better with the use of digital twins.

i. Fog Computing: A decentralized computing architecture known as fog computing puts processing power closer to Internet of Things (IoT) devices. Although though it uses a more distributed methodology, it is comparable to edge computing. For real-time IoT applications, data processing speed and latency reduction are essential, and fog computing can help.
ii. Hybrid Cloud: A hybrid cloud is an infrastructure that combines public and private clouds. IoT networks may balance their needs for affordability, scalability, and security with the aid of hybrid clouds. For instance, private cloud infrastructure can be used to store sensitive data whereas public cloud infrastructure can be used to store less sensitive data.
iii. Human-Machine Interfaces (HMIs): HMIs allow users to communicate with IoT systems and devices. HMIs come in tactile, aural, and visual forms. These could aid in enhancing IoT networks' usability and accessibility.
iv. Predictive Maintenance: In order to forecast when maintenance is necessary before equipment fails, predictive maintenance uses data from IoT sensors. Reduced downtime, increased dependability, and lower maintenance costs can all be a result of predictive maintenance.
v. Smart Energy: To maximize energy efficiency and minimize waste, smart energy utilises IoT networks. IoT sensors, for instance, can be used to track energy use in buildings and modify heating or lighting based on occupancy levels.
vi. Voice Recognition: Voice-activated instructions and IoT device control are made possible by speech recognition technologies. Speech recognition can help make IoT networks more convenient and accessible.

B. Edge computing and 5G networks

The adoption of edge computing and 5G networks is one of the most important trends in IoT networks. Instead of transmitting data to a central server for processing, edge computing uses devices at the network's edge to process data. Many IoT applications depend on low latency and quick reaction times, which can be achieved with this method. Contrarily, 5G networks provide greater bandwidth and lower latency than earlier wireless network generations, making them ideal for Internet of Things (IoT) applications.

C. Artificial Intelligence and Machine Learning

The growing application of machine learning (ML) and artificial intelligence (AI) technology in IoT networks is another trend. IoT devices can benefit from AI and ML to improve decision-making and automate processes like anomaly detection and predictive maintenance. Costs can be cut, productivity can be increased, and the user experience can be improved.

D. Blockchain technology

In IoT networks, blockchain technology is another new development. Blockchain is a distributed ledger technology that makes transactions safe, open, and impenetrable. Blockchain can be utilized in IoT networks to build secure, decentralized systems that are impervious to hackers or tampering. Blockchain technology, for instance, can be applied to develop a safe and open supply chain management system that can monitor the flow of commodities from manufacture to delivery.IoT networks have a promising future, filled with both exciting prospects and difficult obstacles. To ensure that IoT networks can reach their full potential as the technology develops, it will be crucial to solve challenges like privacy, security, and interoperability.

VI. Challenges & Limitations of IoT Network

IoT networks provide many benefits, but they also present a number of obstacles and constraints that need to be overcome. We will look at a few of these difficulties and their potential effects in this section.

A. Privacy and Security Issues

Security and privacy issues are one of the biggest problems facing IoT networks. Given that there are billions of internet-connected gadgets, the possibility of cyberattacks and data breaches is a major worry. IoT devices sometimes have poor security safeguards, which leaves them open to hacking and other online dangers. Furthermore, IoT devices frequently gather and send sensitive data, such private health information, necessitating strong privacy measures.

B. Problems with Interoperability and Compatibility

Interoperability and compatibility problems are another difficulty facing IoT networks. IoT systems and devices are frequently created by several manufacturers and may employ various communication protocols or standards. As a result, integrating equipment from many manufacturers and developing a cohesive system may be difficult. Additionally, the demand for interoperability and compatibility will only increase as IoT networks develop.

C. Congestion in the Network and Scalability

Scalability and network congestion are additional issues that IoT networks must deal with. The need for bandwidth and other network resources increases along with the number of devices connected to the network. This may cause network congestion, which may have an effect on how well IoT applications work. Scaling the network infrastructure to meet the rising demand might be difficult as the number of IoT devices keeps increasing.

D. Battery Life and Power Use

For IoT networks, power consumption and battery life are major obstacles. Many Internet of Things (IoT) devices run on batteries and can be found in far-off or challenging-to-reach places. This makes it difficult to change batteries or recharge devices, which may affect the network's overall dependability and performance. In addition, power consumption will become a more pressing issue as the number of IoT devices increases.IoT networks provide many advantages, but there are also a number of problems and restrictions that need to be worked around. IoT networks may realize their full potential by creating strong security and privacy measures, addressing interoperability and compatibility challenges, managing network congestion, and minimizing power usage.

VII. Conclusion

We have covered the architecture, applications, and anticipated future developments of IoT networks in this paper. We have looked at an IoT network's four-tiered architecture and all of its components, such as sensors, gateways, cloud platforms, and apps. We have also discussed the various applications of IoT networks in a variety of fields, including healthcare, industry, transportation, and even smart cities.We have also looked into the most recent advancements in the Internet of Things (IoT), such as edge computing, 5G networks, AI, and blockchain. The usefulness and value of IoT networks may rise as a result of these tendencies.IoT networks provide a lot of advantages, but they also have some disadvantages that need to be dealt with. This includes problems with energy use, battery life, interoperability, scalability, security, and privacy. It also includes problems with network congestion.To fully realize the potential of IoT networks, future research should focus on fixing these problems and overcoming these limitations. Managing network congestion, optimizing energy use, creating robust security and privacy measures, and resolving interoperability and compatibility issues are a few of them.IoT networks, which have the potential to revolutionize numerous industries and raise people's living standards everywhere, represent a significant advancement in technology. With further research and development, IoT networks will without a doubt play a significant role in determining the direction of technology and society.

References

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[3] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2011). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.

[4] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787-2805.

[5] Wang, S., Zhang, Y., & Zhang, Y. (2019). Fog computing: Platform and applications. Journal of Network and Computer Applications, 123, 1-18.

[6] Ray, P. P. (2016). Internet of things for smart agriculture: Technologies, practices and future direction. Journal of Ambient Intelligence and Humanized Computing, 7(6), 783-798.

[7] Amin, R., & Islam, M. R. (2018). Internet of Things (IoT) based wearable technology for health monitoring: A review of critical issues and challenges. IEEE Sensors Journal, 18(21), 8550-8563.

[8] Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684-700.

[9] He, W., Yan, G., & Da Xu, L. (2014). Developing vehicular data clouds for connected vehicles. IEEE Transactions on Emerging Topics in Computing, 2(1), 23-32.

[10] Hossain, M. S., Muhammad, G., & Alamri, A. (2019). Blockchain-based secure Internet of Things: Challenges and solutions. IEEE Internet of Things Journal, 6(5), 8294-8310.

[11] Li, M., Lu, R., Li, W., & Lin, X. (2018). Secure data sharing in cloud-based Internet of Things via attribute-based encryption. IEEE Transactions on Information Forensics and Security, 13(7), 1755-1767.

[12] Mao, Y., You, I., & Zhang, J. (2012). A survey on security of Internet of Things. International Journal of Communication Systems, 25(9), 1101-1111.

[13] Mohanty, S. P., Prasad, N. R., & Saraju Mohanty, M. (2018). Internet of Things and big data analytics: Foundations, challenges, and future directions. Journal of Parallel and Distributed Computing, 129, 1-24.

[14] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[15] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of things: A survey. Computer networks, 54(15), 2787-2805.

[16] Chen, M., Ma, Y., Song, J., Lai, C. F., & Hu, B. (2018). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. IEEE Transactions on Industrial Informatics, 14(8), 3690-3700.

[17] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[18] Li, Y., & Lu, R. (2018). Blockchain and Internet of Things (IoT): A survey. IEEE Internet of Things Journal, 5(5), 4419-4434.

[19] Liu, X., Chen, Y., Chen, X., Hu, F., & Zhang, W. (2019). An efficient access control scheme for the Internet of Things based on blockchain technology. IEEE Access, 7, 55880-55890.

[20] Mahmud, R., Hu, J., & Miao, Y. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Transactions on Vehicular Technology, 67(8), 6745-6758.

[21] Moosavi, S. R., & Gholami, M. (2019). A comprehensive review on the Internet of Things (IoT) security threats and countermeasures. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1663-1678.

[22] Ning, H., Zou, W., Wei, Z., & Zhang, L. (2019). An energy-efficient and scalable edge computing architecture for internet of things applications. IEEE Transactions on Industrial Informatics, 15(6), 3502-3512.

[23] Peng, T., Li, Z., Li, J., Wang, X., & Wang, Y. (2019). Big data analytics in smart healthcare: A review. Journal of biomedical informatics, 92, 103139.

[24] Qu, W., Zhuang, Y., Chen, M., & Wang, H. (2019). Secure and privacy-preserving data aggregation for internet of things: A survey. IEEE Internet of Things Journal, 6(4), 6506-6523.

DOI: https://doi.org/10.17762/turcomat.v11i3.13604

[25] Rahmani, A. M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., & Adel, M. (2019). Smart homes for elderly healthcare—Recent advances and research challenges. Journal of Ambient Intelligence and Humanized Computing, 10(12), 4515-4536.

[26] Rawat, P., Singh, A., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: A survey on recent developments and potential synergies. The Journal of Supercomputing, 68(1), 1-48.

[27] Shafagh, H., Hithnawi, A., & Duquennoy, S. (2017). Poster: Towards a blockchain-based security framework for the Internet of Things. In Proceedings of the 2017 ACM International Conference on Embedded Networked Sensor Systems (pp. 437-438).

[28] Wang, L., Torkamani, M., Al-Fuqaha, A., & Sattar, F. (2018). From machine-to-machine communications towards cyber-physical systems. IEEE Access, 6, 42381-42398.