INTERNET OF THINGS NETWORK ARCHITECTURE AND SECURITY CHALLENGES

Muhammad R Ahmed[1], Ahmed Al Shihimi [1], Thirein Myo[1] Badar Al Baroomi[1] and M Shamim Kaiser[2]

[1]Military Technological College, Muscat, Oman
[2]Institute of Information Technology , Jahangirnagar Universiry, Savar, Bangladesh

ABSTRACT

The Internet of Things (IoT) has transformed not only the way we communicate and operate our devices, but it has also brought us significant security challenges. A typical IoT network architecture consists of four levels: a device, a network, an application, and a service, each with its own security considerations. There are three types of IoT networks: Personal Area Networks (PANs), Local Area Networks (LANs), and Wide Area Networks (WANs). Each type has its own security requirements, so it is important to understand their particular security requirements. Several communication protocols that are used in IoT networks, like Wi-Fi and Bluetooth, are also susceptible to vulnerabilities that require the implementation of additional security measures. In addition to physical security challenges, there are numerous security challenges in the form of authentication, encryption, software vulnerabilities, DoS attacks, data privacy, and supply chain security. In order to deal with these challenges, we need to take a multi-layered approach that is comprised of physical, technical, and organizational measures. In this paper, we present an overview of IoT network architecture, along with an analysis of security challenges.

KEYWORDS

Internet of Things, Architecture, Challenges, Security

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way in which devices, sensors, and objects communicate and operate by permitting them to be interconnected and operate as a unit through the use of the internet[1], [2]. Despite the technological advances that have brought about the rise of the Internet of Things, there are also significant security challenges that must be addressed in order to ensure the well-being of individuals and the privacy of organizations[3].

In terms of the architecture of an IoT network, there are four different levels: the device layer, the network layer, the application layer, and the service layer[4]. IoT networks are built on layers, each of which plays an important role in their functioning and requires specific considerations in order to maintain their security and privacy. In the case of IoT devices, for example, the device layer includes devices that require the proper mechanisms of authentication, authorization, and encryption in order to facilitate secure communication and data transmission between devices[5].

Furthermore, IoT networks can also be classified into three types based on their characteristics and requirements: Personal Area Networks (PANs), Local Area Networks (LANs), and Wide Area Networks (WANs), each of which has its own characteristics and requirements [6].

David C. Wyld et al. (Eds): ICDIPV, CBIoT, ICAIT, WIMO, NC, CRYPIS, ITCSE, NLCA, CAIML -2023
pp. 171-179, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131313

Typically, PAN networks are used to connect wearable devices and have a low-power consumption requirement, while WAN networks require both long-range and low-power consumption communication protocols in order to operate, such as LoRaWAN [7].

Furthermore, in addition to IoT network architectures, communication protocols used in IoT networks play a significant role in ensuring the security and privacy[8]. Wi-Fi and Bluetooth protocols, for example, are commonly used in PAN and LAN networks, but they present vulnerabilities that need to be addressed in order to ensure network security against cyber threats. Even though IoT networks have many benefits, there are also a number of security challenges that need to be addressed. These challenges include, but are not limited to, physical security, authentication, access control, encryption, software vulnerabilities, denial-of-service attacks, data privacy, and supply chain security[9].

IoT devices could be compromised physically by a number of factors, including theft, tampering, and destruction of the devices, which could compromise the security of the network. There are a number of challenges when it comes to authentication and access control, such as ensuring only authorized users and devices are able to access the network and data, preventing unauthorized access, and maintaining data integrity[10]. In order to ensure that data transmission and storage are secure, encryption is essential for preventing unauthorized access to data. Despite the fact that software vulnerabilities, such as outdated firmware or weak passwords, are isolated, hackers can exploit them to gain access to a network. The DoS attack is another type of attack where an attacker floods the network with traffic so that it cannot operate. Privacy is another important issue for organizations, as sensitive information may be at risk of being intercepted or breached, which could result in privacy violations[11]. There are several security challenges associated with the supply chain of devices, including ensuring that the components and their manufacturers are secure, and ensuring that they are not compromised or contain vulnerabilities. A generic Internet of Things (IoT) network with applications possibilities shown in Figure 1 [12].

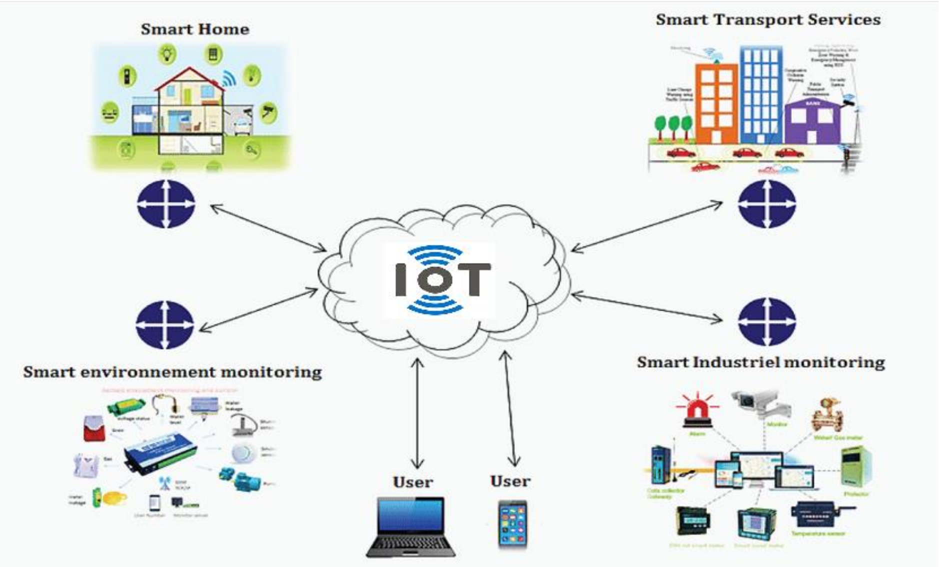

Figure 1. A generic Internet of Things (IoT) network

In order to resolve these challenges, it is necessary to adopt a multi-layered approach which involves implementing technological, organizational, and physical measures to protect against the possibility of security breaches. In order to enhance the security of IoT devices, strong authentication mechanisms, encryption protocols, and regular firmware updates can all be implemented. The organization can also contribute to enhancing the security of IoT networks by taking measures such as implementing security policies, conducting regular audits of security, and training employees in the use of IoT networks.

The Internet of Things (IoT) offers a number of benefits, but they can also present significant security challenges that need to be addressed. The proper use of security measures, including the use of a multilayer approach, can help mitigate these challenges, enabling individuals and organizations to remain safe and protected when using IoT devices. In light of the rapidly growing use of IoT devices, it is essential to address these challenges proactively and ensure users continue to have trust in this transformative technology.

2. IOT ARCHITECTURE

There is a widely used framework for the design and implementation of IoT systems that is based on the four-layer model of IoT systems. There is a structured approach to understand the different components of an IoT system, and how they interact with one another as part of an IoT system[13], [14]. The four layer architecture are shown in the Figure 2.

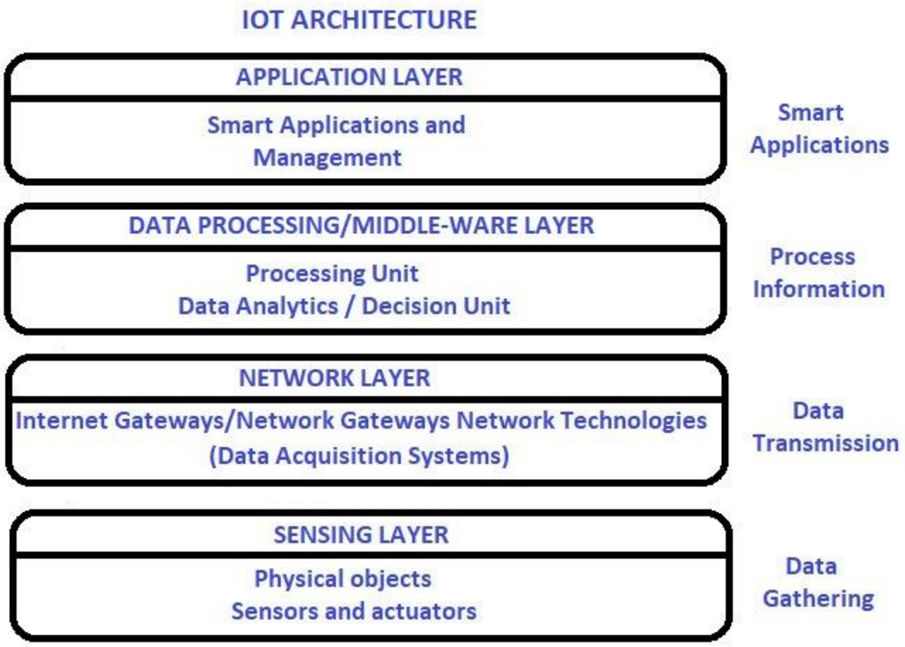

Figure 2. The IoT four layer atchitecture

- A perception layer, also known as the physical layer or sensing layer of the IoT architecture, is the lowest component of the IoT architecture. Sensors and actuators are part of the physical device layer of the data collection system. They collect the data by collecting it from the surrounding environment. In this layer, the devices in the physical world are able to perceive and sense the physical world and acquire data, which is then transmitted back to the network layer.
- In the network layer, the devices are connected to each other through the use of Ethernet cables and they can also access the internet. There are several layers within the networking architecture, but the network layer comes to play the most important role in setting up the infrastructure for communication and storage of data. Networks of different types, such as LANs,

WANs, and PANs, can be used in the network layer as a means of facilitating communication between the devices.

- As a bridge between perception and application, the middleware layer serves as a link between the two layers. A communication protocol is handled by it, as well as data storage and security features of the Internet of Things system. The middleware layer is responsible for integrating devices and networks, providing a platform for the development of IoT applications and enabling the integration of multiple devices and networks.
- The application layer is the top layer of the IoT architecture and is responsible for providing the end-users with an interface to interact with the IoT system. Various types of applications can be found in this layer, including data acquisition applications, data processing applications, and data presentation applications. These applications are able to collect the data from the devices, analyze the data, and then present the result of that analysis to the end users in a meaningful way.

An important advantage of the four-layer IoT architecture model is its modularity and flexibility, which is a significant benefit of its design. It is also possible to optimize and tailor each layer of the architecture so that it can be tailored to the specific requirements, which allows the architecture to be scalable, interoperable, and secure[15]. Furthermore, because of the modular nature of the IoT architecture model, it is possible to develop and deploy new IoT applications and services.

Despite this, there are several challenges associated with the four-layer IoT architecture. There is a critical challenge to ensuring the security and privacy of the data collected by the Internet of Things system. In order to ensure that the IoT systems do not fall target to cyber attacks, it is imperative that appropriate security measures are implemented at each layer of the architecture[16]. As part of the challenge, it is also necessary to ensure the interoperability between different devices and networks that use different communication protocols and data formats.

IoT architectures can be divided into four layers based on their functions and provide a structured and flexible approach to designing and implementing IoT systems. There are many layers in the IoT architecture, and each of them plays a crucial role in the functioning of the IoT system, and optimizing each layer can result in a more reliable and efficient IoT system. IoT presents significant challenges for securing the system and making it interoperable. These are critical issues that must be addressed in order for the IoT to be able to realize its full potential.

3. Types of IoT Networks

There have been various types of Internet of Things (IoT) networks developed in recent years that enable devices to communicate and exchange data with each other. The characteristics, advantages, and limitations of each type of IoT network allow it to be suitable for a variety of different applications. IoT networks can be divided into various types depending on their purpose and include[17], [18].

- Wireless Personal Area Networks (WPANs): A WPAN is a type of wireless network that allows devices to communicate with each other wirelessly over a short range, usually from a few meters to a few meters or less. Bluetooth and Zigbee are two technologies that are examples of WPAN technologies. WPANs are commonly used for home automation, personal health monitoring, and wearable devices.
- Wireless Local Area Networks (WLANs): Wireless Local Area Networks (WLANs) are networks that use wireless technology to cover a large area, such as a building or a campus. The

wireless local area network (WLAN) utilizes Wi-Fi technology to provide high-speed connectivity to IoT devices. A Wireless Local Area Network (WLAN) is commonly used in home automation, smart cities, and industrial automation.

- Wireless Wide Area Networks (WWANs): Wireless Wide Area Networks (WWANs) are a type of wireless network that spans a wide geographical area and is designed to connect devices in IoT across long distances. Several wireless technologies are used in the field of wide area networks, such as 4G and 5G. WWANs are one of the most commonly used technologies in transportation, logistics, and environmental monitoring.
- Low-Power Wide Area Networks (LPWANs): LPWANs are designed as a way to provide long-range connectivity to IoT devices by using a minimal amount of power. A low-power wide area network (LPWAN) uses a wide variety of technologies, such as LoRaWAN and Sigfox, and these are commonly used in smart agriculture, smart buildings, and smart cities.
- Satellite Networks: In addition to providing broadband coverage worldwide, satellite networks may also be utilized in special applications where terrestrial networks are not feasible or available, such as maritime, aviation, and remote locations. In spite of this, satellite networks are expensive and have a high level of latency, which makes them unsuitable for applications that require real-time communication.
- Power Line Communication (PLC) Networks: The use of power lines in PLC networks enables the transmission of data between devices. A PLC network is one of the most commonly used kinds of networks in smart homes as well as smart grid applications.

Regardless of the type of IoT network that is used, each type of network has its own characteristics, advantages, and limitations. An application's choice of network depends on the specifics of the application, the range of coverage required, the bandwidth requirements, the latency requirements, and the power consumption limitations of the devices. It is expected that as new technologies are developed, and as the demand for IoT applications increases, IoT networks will continue to evolve.

4. COMMUNICATION PROTOCOLS OF IOT NETWORKS

The protocol that facilitates the transfer of data between devices is crucial in the functioning of any IoT network, as it facilitates the transfer of data between devices. In order to meet the requirements of various IoT applications and use cases, bandwidth, latency, and power consumption vary to a great extent, leading to the development of a number of communication protocols. There are a number of different communication protocols used in IoT networks, and some of the most commonly used ones include[19], [20].

- MQTT (Message Queuing Telemetry Transport): This is a lightweight, publish-subscribe messaging protocol that is widely used in the field of Internet of Things applications. It is designed for low-bandwidth, high-latency networks and has a small footprint, which makes it suitable for use on resource-constrained devices.
- CoAP (Constrained Application Protocol): This application-layer protocol is designed to be lightweight and easily adapted to devices that have limited memory and processing power. It is based on a client-server architecture and provides a RESTful interface for the exchange of data between devices.
- HTTP (Hypertext Transfer Protocol): The purpose of this protocol is to allow communication between web servers and clients. As part of the Internet of Things, HTTP is used in the context of providing a web interface for accessing and controlling IoT devices.
- Zigbee: This low-power wireless protocol is designed for low-bandwidth applications. In the 2.4 GHz frequency band, Zigbee is a wireless communication technology commonly used in the field of home automation and industrial control systems.

- LoRaWAN (Long Range Wide Area Network): Designed for long-range connectivity, LoRaWAN is a low-power, wide-area network protocol for IoT devices. The LoRaWAN technology is based on unlicensed subGHz frequency bands and it is capable of providing connectivity over distances of several kilometers.
- BLE (Bluetooth Low Energy): This wireless protocol is designed for low-power devices. There are a number of applications that utilise Bluetooth Low Energy, such as wearables and smart home applications.
- NFC (Near Field Communication): A short-range wireless communication protocol to exchange data between devices in proximity. It is common for NFC to be used in payment systems and access control applications.

There is a variety of communication protocols that can be used for IoT applications, depending on the specific requirements of the application, such as the range of coverage, the data rate, and the power consumption limitations of the devices. As part of the design and implementation of IoT systems, the interoperability of different devices and networks that use different communication protocols is also an important consideration to consider when designing and implementing IoT systems.

5. CHALLENGES

A number of challenges are involved with the development of an IoT network architecture, including those related to scalability, interoperability, security, and privacy. There is going to be a huge number of devices connected to the IoT network which will require the development of a scalable network architecture that can handle the increased traffic. Interoperability between devices that use different protocols is another major challenge that needs to be addressed. Security and privacy are also significant concerns in the IoT world, considering the fact that these devices may be prone to cyber attacks. In the field of internet of things networks, there are a number of security challenges that must be addressed in order to ensure the safety and privacy of both the devices and the data they generate. A few of the challenges associated with security include[21]–[23]: Figure 3 shows the typical IoT security challenges.

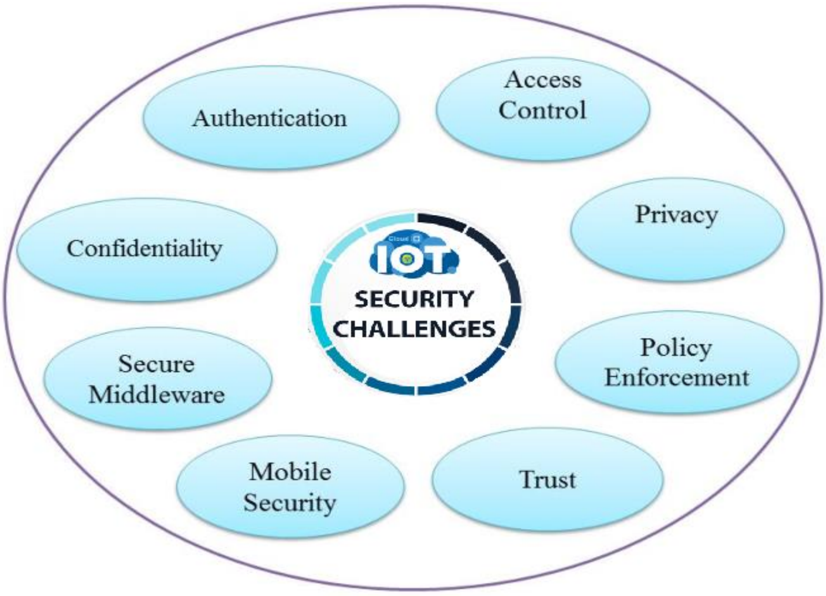

Figure 3. Typical IoT Security Challenges

- Physical security: The Internet of Things is often deployed in public places and, as a result, they are typically at risk of physical tampering, theft, or vandalism. Attackers have the ability to manipulate the physical device in order to gain access to the data it stores or even to control it. It is possible for an attacker to take advantage of an IoT device that is legitimate and replace it with a malicious one that can be used to infiltrate a network. The use of physical security measures such as tamper-evident seals, locks, and alarms is one way of mitigating such risks.
- Authentication and access control: Internet of Things devices are often connected to the internet and can be accessed from anywhere in the world. In order to prevent unauthorized access to and data breaches, it is important to have strong authentication and access control mechanisms in place to prevent these breaches. The problem with weak or default passwords is that the attackers are often able to gain access to a multitude of IoT devices. The use of two-factor authentication, the use of access control lists, and the use of secure communication protocols can help prevent these types of attacks.
- Encryption: The Internet of Things generates and transmits sensitive data, such as personal and financial information, which must be protected from interception and eavesdropping. Various encryption technologies, such as SSL/TLS, AES, and RSA, can provide secure communication between devices connected to the Internet of Things as well as servers. Unless IoT devices are properly encrypted, the data transmitted by them may be easily intercepted, resulting in serious data breaches.
- Software vulnerabilities: It is common for IoT devices to use off-the-shelf components and these components might contain software vulnerabilities which can be exploited by hackers. It is important to keep your software updated and patched in order to mitigate these risks. The problem with IoT devices is that they are rarely updated on a regular basis, leaving them open to attacks. There are a number of vulnerabilities that can be exploited by attackers, such as buffer overflows, SQL injections, and cross-site scripting, to gain access to the device or network.
- Denial of Service (DoS) attacks: It is possible to target IoT devices with a DoS attack, which can overwhelm the network and disrupt communication between the devices. This type of attack involves flooding the network with a large volume of traffic, resulting in the network becoming unusable for legitimate users. In order to prevent DoS attacks, traffic filtering should be implemented as well as reducing the number of connections to help prevent DoS attacks.
- Data privacy: Internet of Things networks generate vast amounts of data, and it is possible to use this data to track individuals and their behavior. These data can be used by attackers as a means of gaining unauthorized access to sensitive information and can also be used for malicious purposes. There are several privacy measures that can assist in protecting the privacy of the individuals, such as anonymization and data minimization.
- Supply chain security: A number of IoT devices are manufactured and assembled in different parts of the world, which can make it difficult to ensure the security of the supply chain. There are vulnerabilities that can be exploited in the supply chain by attackers to gain unauthorized access to devices or introduce malicious components. A number of security measures can be applied to the supply chain in order to mitigate risks, such as verifying that components are genuine and implementing security audits, in order to mitigate these risks.

To address these challenges in terms of security, it is necessary to implement a multilayered approach that involves physical, technical, and organizational measures. There is a need to incorporate security and privacy considerations into the design and implementation of IoT networks in order to ensure their safety and reliability.

6. CONCLUSIONS

IoT, as a result of its rapid growth, promises to have a profound impact on how we interact with our environment. The success of the Internet of Things depends on the availability of a reliable and efficient network architecture that can support the massive number of devices that will be connected to it. It provided a comprehensive overview of IoT network architectures and the challenges associated with them. IoT can only achieve its full potential through ongoing research and development. A network architecture for the Internet of Things has four layers: the device layer, the network layer, the application layer, and the service layer. The Internet of Things can be classified into three types: Personal Area Networks (PAN), Local Area Networks (LAN), and Wide Area Networks (WAN). Communication protocols used in IoT networks include Wi-Fi, Bluetooth, Zigbee, and LoRaWAN. There are several security challenges associated with IoT networks, including physical security, authentication and access control, encryption, software vulnerabilities, DoS attacks, data privacy, and supply chain security. Managing these challenges requires implementing physical, technical, and organizational measures. The design and implementation of IoT networks must incorporate security and privacy considerations to ensure their safety and reliability. In future we will be implementing the security mechanisms based on anomaly of the network.

REFERENCES

[1] K. O. M. Salih, T. A. Rashid, D. Radovanovic, and N. Bacanin, “A Comprehensive Survey on the Internet of Things with the Industrial Marketplace,” Sensors, vol. 22, no. 3, Art. no. 3, Jan. 2022, doi: 10.3390/s22030730.

[2] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, “Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk,” IEEE Access, vol. 7, pp. 129551–129583, 2019, doi: 10.1109/ACCESS.2019.2932609.

[3] C. Maple, “Security and privacy in the internet of things,” Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, May 2017, doi: 10.1080/23738871.2017.1366536.

[4] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of Internet of Things,” in 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Aug. 2010, pp. V5-484-V5-487. doi: 10.1109/ICACTE.2010.5579493.

[5] M. Saqlain, M. Piao, Y. Shim, and J. Y. Lee, “Framework of an IoT-based Industrial Data Management for Smart Manufacturing,” Journal of Sensor and Actuator Networks, vol. 8, no. 2, Art. no. 2, Jun. 2019, doi: 10.3390/jsan8020025.

[6] G. Pau, C. Chaudet, D. Zhao, and M. Collotta, “Next Generation Wireless Technologies for Internet of Things,” Sensors, vol. 18, no. 1, Art. no. 1, Jan. 2018, doi: 10.3390/s18010221.

[7] R. C. Braley, I. C. Gifford, and R. F. Heile, “Wireless personal area networks: an overview of the IEEE P802.15 working group,” SIGMOBILE Mob. Comput. Commun. Rev., vol. 4, no. 1, pp. 26–33, Jan. 2000, doi: 10.1145/360449.360465.

[8] S. Kraijak and P. Tuwanut, “A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends,” in 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), Sep. 2015, pp. 1–6. doi: 10.1049/cp.2015.0714.

[9] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” in 2015 IEEE Symposium on Computers and Communication (ISCC), Jul. 2015, pp. 180–187. doi: 10.1109/ISCC.2015.7405513.

[10] B. Russell and D. V. Duren, Practical Internet of Things Security. Packt Publishing Ltd, 2016.

[11] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, “Identifying the attack surface for IoT network,” Internet of Things, vol. 9, p. 100162, Mar. 2020, doi: 10.1016/j.iot.2020.100162.

[12] Z. Abbas and W. Yoon, “A Survey on Energy Conserving Mechanisms for the Internet of Things: Wireless Networking Aspects,” Sensors, vol. 15, no. 10, Art. no. 10, Oct. 2015, doi: 10.3390/s151024818.

[13] M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "IoT Architecture," in Towards the Internet of Things: Architectures, Security, and Applications, M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, Eds., in EAI/Springer Innovations in Communication and Computing. Cham: Springer International Publishing, 2020, pp. 9–31. doi: 10.1007/978-3-030-18468-1_2.

[14] C.-L. Zhong, Z. Zhu, and R.-G. Huang, "Study on the IOT Architecture and Gateway Technology," in 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), Aug. 2015, pp. 196–199. doi: 10.1109/DCABES.2015.56.

[15] K. Yelamarthi, M. S. Aman, and A. Abdelgawad, "An Application-Driven Modular IoT Architecture," Wireless Communications and Mobile Computing, vol. 2017, p. e1350929, May 2017, doi: 10.1155/2017/1350929.

[16] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," J Big Data, vol. 6, no. 1, p. 111, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[17] S. Oza et al., "IoT: The Future for Quality of Services," in ICCCE 2019, A. Kumar and S. Mozar, Eds., in Lecture Notes in Electrical Engineering. Singapore: Springer, 2020, pp. 291–301. doi: 10.1007/978-981-13-8715-9_35.

[18] D. Sehrawat and N. S. Gill, "Smart Sensors: Analysis of Different Types of IoT Sensors," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Apr. 2019, pp. 523–528. doi: 10.1109/ICOEI.2019.8862778.

[19] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in 2017 8th International Conference on Information Technology (ICIT), May 2017, pp. 685–690. doi: 10.1109/ICITECH.2017.8079928.

[20] I. Heđi, I. Špeh, and A. Šarabok, "IoT network protocols comparison for the purpose of IoT constrained networks," in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), May 2017, pp. 501–505. doi: 10.23919/MIPRO.2017.7973477.

[21] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," in 2021 26th International Conference on Automation and Computing (ICAC), Sep. 2021, pp. 1–6. doi: 10.23919/ICAC50006.2021.9594183.

[22] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.

[23] H. Lin and N. W. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," Information, vol. 7, no. 3, Art. no. 3, Sep. 2016, doi: 10.3390/info7030044.