IoT SECURITY OF EDGE COMPUTING

H.H. Sudani

Iraqi Ministry of Science and Technology, Baghdad, Iraq

IoT is a mesh of physical things or objects that are connected to the Internet. These objects interconnect with external and internal environments with the help of embedded technology. Physical things analyze sense, control, and decide independently or in alliance with other things by way of two-way communication and high-speed control. This is also essential for the smart grid [1]. IoT results from current progress in embedded processing, wireless, and sensing technologies. IoT-based smart grids need six fundamental technologies, which include software-defined objects, model protocols, edge computing-based analysis, intelligent sensing, low cost, and network information security. One of the vital challenges for IoT is managing the large amount of data produced by sensors. Sending this massive amount of data directly to the cloud will create problems of latency, security, privacy, and high bandwidth utilization. On the other hand, its hasty development leads to the neglect of security threats to a large extent in edge computing platforms and their enabled applications.

Edge computing (EC) is the major technology to attain real-time demand response for IoT-based smart grids [2]. EC carries out computation at the edge of the network. It emphasizes being near the user and the data source. It is real-time, reliable, and faster.

Thus, privacy protection needs to be considered in edge computing, and effective privacy-preserving mechanisms such as local differential privacy and differential privacy with high utility [3] need to be designed to protect the privacy of users in the edge computing-based IoT environment. IoT gateways and security solutions help address the security issues of IoT edge devices. By moving security functionality to the network edge and providing security directly to IoT devices, these solutions help to identify and block potential threats there, improving the overall security posture. In order to provide reliable protection against security threats and attacks, a light-weight authentication scheme needs to be modeled where the EC servers authenticate the end devices without any time delay.

References

1. Meng, W. Smart Grid Neighborhood Area Networks: a Survey / W. Meng, R. Ma, H. H. Chen // IEEE Network. – 2014. – Vol. 28, no. 1. – P. 24–32.

2. Internet of Things Based Smart Grids Supported by Intelligent Edge Computing / S. H. Chen [et al.] // IEEE Access. – 2019. – Vol. 7. – Article ID 74089.

3. On Binary Decomposition Based Privacy-Preserving Aggregation Schemes in Real-Time Monitoring Systems / X. Yang [et al.] // IEEE Trans. Parallel Distrib. Syst. – 2016. – Vol. 27, no. 10. – P. 2967–2983.