Wireless Sensor Networks in Progress of Smart E-Health and Cloud Computation Era

Fatemeh Rabeifar (PhD)[1]*

[1]Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran

Dear Editor,

Wireless sensor networks, as an opening up new opportunities in medical science, have a promising future. The emergence of Smart E-Health, driven by the Internet of Things (IoT), has facilitated the development of intelligent healthcare [1].

Further, a wireless sensor network comprises independent sensors distributed at specific intervals, working together to monitor physical or environmental parameters. Each node within the network is equipped with a sensor, microcontroller, radio transmitter, and energy-saving element [2].

Wearable sensors for patients are often organized into simplified wireless networks due to time limitations [3]. Gateways and high security, as challenges, are needed. Web-based technologies, such as the semantic web, service-oriented processing, and cloud computing have facilitated global communication within virtual medical organizations. Consequently, an intelligent healthcare system first aims to remotely monitor patients in a safe and secure environment, involving leveraging the Internet of Things as a network of interconnected devices, in which data are transmitted through wireless connections to a central processor in the cloud and then shared accordingly.

Architecture of Interconnected Intelligent Things in the Internet of Things: [4]

The present letter explores the architecture of interconnected intelligent things within the IoT framework, with a focus on wireless sensor network technology, and specifically examines the security in the IoT's three-layered structure for intelligent healthcare systems, according to the following sentences:

1. Sensor Layer: Ensuring security in sensors and RFID receivers.
2. Network Layer: Addressing security in network nodes, network infrastructure, and communication protocols.
3. Application Layer: Incorporating environmental monitoring, intelligent information transmission services, and cloud computation.

Further, the collected data from the nodes include the following information:

- Sensor, battery power data, and network and sensor graphs.
- Packets received or destroyed within the networks, neighboring nodes, and routing criteria.

*Corresponding author:
Fatemeh Rabeifar
Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran
E-mail:
rabeifar.f@gmail.com

Received: 4 July 2023
Accepted: 8 August 2023

Recommended Secure Architecture:

In the IoT, a secure architecture is recommended to establish robust security, which requires the following steps for each layer in the three-layered architecture:

1. Sensor Layer: Implementing light encoding technology and protecting sensor data.
2. Network Layer: Identity authentication, encoding mechanisms, and telecommunication security.
3. Application Layer: Identity authentication, privacy protection, security management, and secure cloud computation.

Cloud Computation:

This paradigm can combine wireless sensor networks with real-time data sharing and analysis capabilities for passing sensors. Cloud computation can be also employed to meet the high-level security requirements of intelligent healthcare systems. The convergence of robotic services and cloud processes can increase a new field, known as cloud robotics [5].

Conflict of Interest

None

References

1. Masengo Wa Umba S, Abu-Mahfouz AM, Ramotsoela D. Artificial Intelligence-Driven Intrusion Detection in Software-Defined Wireless Sensor Networks: Towards Secure IoT-Enabled Healthcare Systems. *Int J Environ Res Public Health.* 2022;**19**(9):5367. doi: 10.3390/ijerph19095367. PubMed PMID: 35564763. PubMed PMCID: PMC9103430.
2. Lăzăroiu G, Andronie M, Iatagan M, Geamănu M, Ștefănescu R, Dijmărescu I. Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the internet of manufacturing things. *ISPRS Int J Geo-Inf.* 2022;**11**(5):277. doi: 10.3390/ijgi11050277.
3. Kim YH, Chou D, Lee B, Danilovich M, Lazar A, Conroy DE, Kacorri H, Choe EK. Mymove: Facilitating older adults to collect in-situ activity labels on a smartwatch with speech. CHI Conference on Human Factors in Computing Systems; New York, NY, United States: Association for Computing Machinery; 2022. p. 1-21.
4. Lake D, Milito R, Morrow M, Vargheese R. Internet of things: Architectural framework for ehealth security. *Journal of ICT.* 2014;**1**(3):301-28. doi: 10.13052/jicts2245-800X.133.
5. Rabeifar F, Radfar R, Toloie Eshlaghy A. Cloud Robotic for Development of Smart Telemedicine. *J Biomed Phys Eng.* 2022;**12**(3):225-6. doi: 10.31661/jbpe.v0i0.2202-1465. PubMed PMID: 35698537. PubMed PMCID: PMC9175123.

Citation: Rabeifar F. Wireless Sensor Networks in Progress of Smart E-Health and Cloud Computation Era. *J Biomed Phys Eng*. 2023;13(5):495-496. doi: 10.31661/jbpe.v0i0.2307-1637.