EDITORIAL

Principales desafíos y oportunidades de los sistemas de Internet de las cosas médicas - IoMT

Jorge Gómez Gómez - PhD
Editor Revista Ingeniera e Innovación

En la actualidad hay millones de dispositivos IoT que utilizan las personas para la atención médica. Un IoT con dispositivos médicos se le conoce también como Internet de las cosas médicas (Internet of Medical Things - IoMT). Existen diversas aplicaciones IoMT como (Gómez et al., 2016; Alsubaei, et al., 2019; Basatneh et al., 2018; Nayyar et al., 2019; Pustokhina et al., 2019) entre otras. Los escenarios donde se utiliza esta tecnología son: asistencia a signos vitales de pacientes; monitoreo de información sanitaria; monitoreo en la ingesta de alimentos; monitoreo de señales patológicas y fisiológicas; asistencia al personal sanitario; autogestión, bienestar y prevención; seguimiento de enfermedades entre otras. Todos estos sistemas se enfrentan a algunos desafíos y oportunidades, como se describirán a continuación:

Desafíos

- Privacidad: El primer reto para estos sistemas es la privacidad y la seguridad. La seguridad de los datos almacenados, la privacidad de los datos relacionados con la salud de las personas y la propiedad de los datos de las personas. Este tipo de información tiende a ser la favorita de los Hackers en cualquier lugar del mundo. Para todos no es un misterio que la información relacionada con la salud de las personas es muy sensible, por tanto se convierte en la principal vulnerabilidad de los sistemas IoMT, la cual hay que proteger a como dé lugar; sin embargo no es una tarea fácil y está en constante evolución.
- Almacenamiento de datos: Los métodos seguros de almacenamiento de datos, contienen un mecanismo de control de acceso, como el control de acceso basado en roles. Existen amenazas a la seguridad del análisis de datos que incluyen amenazas a la seguridad en los dispositivos de IoMT como por ejemplo ataque físico, ataque de inyección de información SQL, denegación de servicios entre otros. También hay otros tipos de amenazas como la seguridad en las redes; amenazas de seguridad en dispositivos de la nube como por ejemplo ataque de denegación de servicio distribuido.

También hay otros desafíos como:

- Colaboraciones entre sistemas de computación de borde heterogéneos
- Combinación de fuentes de información heterogéneas
- Abstracción de datos para combinar la representación de datos y operaciones
- Soporte de aplicaciones en tiempo real
- Arquitectura escalable
- Ahorro de energía
- Supervisión del rendimiento
- Confiabilidad de los dispositivos en red en una red altamente distribuida

Oportunidades

- Descarga de cálculos: Este es el proceso para ejecutar un trabajo fuera del dispositivo cuando los recursos del dispositivo son limitados. (Adams y Agesen, 2006; Xian et al.,2007)
- Virtualización ligera: la virtualización proporciona un entorno de máquina virtual para que el

cálculo de descarga cumpla con el requisito de tenencia múltiple. La virtualización ligera ocupa menos espacio y tiempo de memoria (Vaughan, 2006; Alves et al., 2020; Narayanan et al.,2020).

- Redes definidas por software (SDN): SDN permite configurar dinámicamente la red y se puede aplicar a escenarios de computación de frontera. (Mohammed et al., 2020).
- Software de código abierto para desarrollar aplicaciones bioinformáticas (Rafique et al., 2020).

1. Gómez, J., Oviedo, B., & Zhuma, E. (2016). Patient monitoring system based on internet of things. Procedia Computer Science, 83, 90-97.
2. Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. Internet of Things, 8, 100123.
3. Basatneh, R., Najafi, B., & Armstrong, D. G. (2018). Health sensors, smart home devices, and the internet of medical things: an opportunity for dramatic improvement in care for the lower extremity complications of diabetes. Journal of diabetes science and technology, 12(3), 577-586.
4. Nayyar, A., Puri, V., & Nguyen, N. G. (2019). BioSenHealth 1.0: a novel internet of medical things (IoMT)-based patient health monitoring system. In International Conference on Innovative Computing and Communications (pp. 155-164). Springer, Singapore.
5. Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.
6.
7. Adams K, Agesen O (2006) A comparison of software and hardware techniques for x86 virtualization. In: International conference on architectural support for programming languages and operating systems, pp 2–13
8. Xian C, Lu Y-H, Li Z (2007) Adaptive computation offloading for energy conservation on battery-powered systems. In: International conference on parallel and distributed systems, pp 1–8
9. Vaughan-Nichols, S. J. (2006). New approach to virtualization is a lightweight. Computer, 39(11), 12-14.
10. Alves, M. P., Delicato, F. C., Santos, I. L., & Pires, P. F. (2020). LW-CoEdge: a lightweight virtualization model and collaboration process for edge computing. World Wide Web, 23(2), 1127-1175.
11. Narayanan, V., Huang, Y., Tan, G., Jaeger, T., & Burtsev, A. (2020, March). Lightweight kernel isolation with virtualization and VM functions. In Proceedings of the 16th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (pp. 157-171).
12. Mohammed, A. H., KHALEEFAH, R. M., & Abdulateef, I. A. (2020, June). A Review Software Defined Networking for Internet of Things. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-8). IEEE.
13.
14. Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1761-1804.