JEMTAC
Journal of Emergency Medicine Trauma & Acute Care
A PEER REVIEWED JOURNAL

OPEN ACCESS

Qatar Health 2021 Conference

Cybersecurity for next generation healthcare in Qatar

Mohammad Zubair[1,*], Devrim Unal[1], Abdulla Al-Ali[2], Thomas Reimann[3], Guillaume Alinier[3,4,5]

[1]Kindi Center of Computing Research Qatar University, Doha, Qatar
[2]Computer Science and Engineering Department, Qatar University, Doha, Qatar
[3]Hamad Medical Corporation Ambulance Service, Doha, Qatar
[4]School of Health and Social Work, University of Hertfordshire, Hateld, UK
[5]Weil Cornell Medicine-Qatar, Doha, Qatar

*Email: mohammed.zubair@qu.edu.qa

ABSTRACT

Background: IoMT (Internet of Medical Things) devices (often referred to IoMT domain) have the potential to quickly diagnose and monitor patients outside the hospital by transmitting information through the cloud domain using wireless communication to remotely located medical professionals (user domain). Figure 1 shows the proposed IoMT framework designed to improve the privacy and security of the healthcare infrastructure.

Methods: The framework consists of four modules:

1. Intrusion Detection System (IDS)[1] using deep learning (DL) to identify bluetooth-based Denial-of-Service (DoS)-attacks on IoMT devices and is deployed on edge-computing to secure communication between IoMT and edge.
2. IDS[1] is backed up with identity-based cryptography to encrypt the data and communication path.
3. Besides the identity-management system (to authenticate users), it is modeled with aliveness detection using face authentication techniques at the edge to guarantee the confidentiality, integrity, and availability (CIA) of the framework.
4. At the cloud level, another IDS[2] using MUSE (Merged-Hierarchical-Deep-Learning-System-with--Layer-Reuse) is proposed to protect the system against Man-In-The-Middle attacks, while the data is transferred between IoMT-EDGE-CLOUD.

Results: These four modules are developed independently by precisely analyzing dependencies. The performance of IDS[3] in terms of precision is 99% and for the identity-management system, the time required to encrypt and decrypt 256-bit key is 66 milliseconds and 220 milliseconds respectively. The true positive rate is 90.1%, which suggests real-time detection and authentication rate. IDS (2) using MUSE (12-layer) the accuracy is $>95\%$, and it consumes 15.7% to 27.63% less time to train than the smaller four-layer model.

Conclusion: Our designed models suit edge devices and cloud-based cybersecurity systems and support the fast diagnosis and care required by critically ill patients in the community.

Keywords: data security, deep learning, intrusion detection system, user authentication, internet of medical things

http://dx.doi.org/jemtac.2021.qhc.41

QSCIENCE
HAMAD BIN KHALIFA UNIVERSITY PRESS

Cite this article as: Zubair M, Unal D, Al-Ali A, Reimann T, Alinier G. Cybersecurity for next generation healthcare in Qatar, *Journal of Emergency Medicine, Trauma & Acute Care* 2021:41 http://dx.doi.org/jemtac.2021.qhc.41

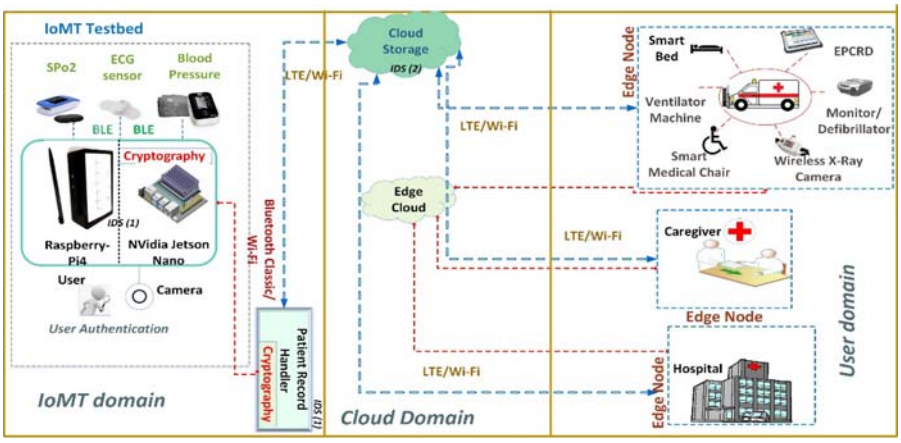

Figure 1. Architecture of the e-health system

Disclosures and acknowledgements: This publication was made possible by NPRP grant NPRP10-0125-170250 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] Zubair M, Unal D, Al-Ali A, Shikfa A. Exploiting Bluetooth Vulnerabilities in e-Health IoT Devices. In: Proceedings of the 3rd International Conference on Future Networks and Distributed Systems; 2019 Jul 1; pp. 1–7.
[2] Hady AA, Ghubaish A, Salman T, Unal D, Jain R. Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. *IEEE Access*. 2020;8:106576–84.
[3] Salman T, Ghubaish A, Unal D, Jain R. Safety Score as an Evaluation Metric for Machine Learning Models of Security Applications. *IEEE Networking Letters*. 2020;2(4): 207–211.