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

OPEN ACCESS

Qatar Health 2022 Conference

Fuzzy Identification-Based Encryption for healthcare user face authentication

Mahima Aggarwal[1], Mohammed Zubair[1,2], Devrim Unal[1,*], Abdulla Al-Ali[2], Thomas Reimann[3,4], Guillaume Alinier[3,5,6,7]

[1]KINDI Center for Computing Research, College of Engineering, Qatar University, Doha, Qatar
[2]Department of Computer Science and Engineering, College of Engineering, Qatar University, Doha, Qatar
[3]Hamad Medical Corporation Ambulance Service, Doha, Qatar
[4]Jacksonville State University, Alabama, USA
[5]School of Health and Social Work, University of Hertfordshire, Hatfield, UK
[6]Weill Cornell Medicine-Qatar, Doha, Qatar
[7]Faculty of Health and Life Sciences, Northumbria University, Newcastle upon Tyne, UK
*Email: dunal@qu.edu.qa

ABSTRACT

Background: Internet of Medical Things (IOMT) has the potential to monitor health continuously and in real-time. One of the main issues that arise in IOMT is how securely the data can be transmitted to the clinical team. In this project, biometric Identity-based encryption was utilized using the Fuzzy-IBE (Identity-based encryption) scheme that uses face features of the clinicians to create the public key. Figure 1 shows the testbed setup designed to improve the privacy and security of the patients' healthcare data.

Methods: The testbed comprises an ESP32 platform sensing and encrypting data, the Nvidia Jetson Nano for data collection and decryption, and the Thingsboard online platform for vital information visualization. Fuzzy Identity-Based Encryption (FIBE)[1−3] uses legitimate users' facial features. The encrypted vital information is transmitted to the Edge-device (Jetson Nano) through BLE/Wi-Fi. On the edge-device of the healthcare system, the face authentication mechanism verifies the user's (clinician) legitimacy to assess the data. Upon user authentication, their facial features will be used to generate a private decryption key that can decrypt the received encrypted data. The data is further sent to the core cloud (Thingsboard) for storage and visualization. To secure the data on the cloud, we deployed an Intrusion Detection System (IDS) model using deep learning to identify the inter-domain stream of malicious traffic.

Results: The face authentication testing using Fuzzy Identity-based Cryptography relied on a public data set. The execution time was calculated for Encryption (time to encrypt the patient's vital data using a public key of health physician's facial features) and decryption (time to match at least d components of the ciphertext and perform message decryption). The experimental results are reported in Table 1.

Conclusion: In today's age of advanced telecommunication technology, cyber security is a very important factor. The designed testbed setup in this work showcases how healthcare data can be secured against malicious attacks.

Keywords: Fuzzy Identity based Encryption, Deep Learning, Face biometry, user authentication, Internet of Medical Things

http://dx.doi.org/10.5339/jemtac.2022.qhc.72

Submitted: 27 July 2021
Accepted: 15 September 2021
Publication date: 15 January 2022

© 2022 Aggarwal, Zubair, Unal, Al-Ali, Reimann, Alinier, licensee HBKU Press. This is an open access article distributed under the terms of the Creative Commons Attribution license CC BY-4.0, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

Cite this article as: Aggarwal M, Zubair M, Unal D, Al-Ali A, Reimann T, Alinier G. Fuzzy Identification-Based Encryption for healthcare user face authentication, *Journal of Emergency Medicine, Trauma & Acute Care* **2022:72** http://dx.doi.org/10.5339/jemtac.2022.qhc.72

كيوساينس
QSCIENCE
دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS

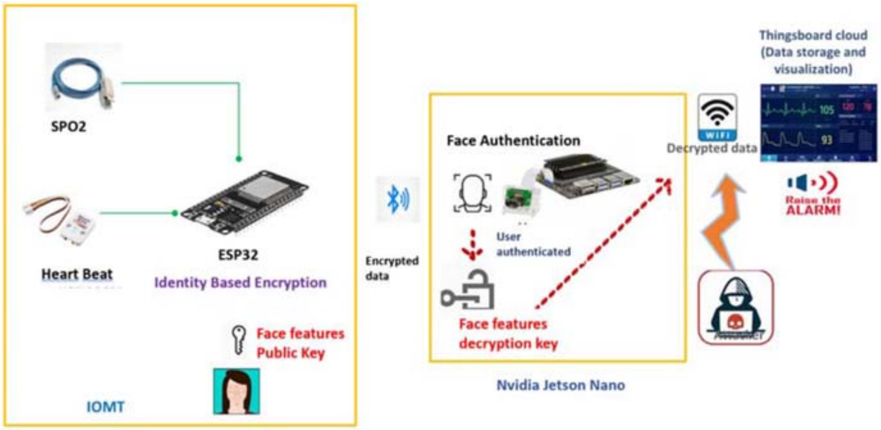

Figure 1. Testbed setup to showcase security of health data before it is sent to the core cloud (based on current data transmission process).

Table 1. Time taken (s) by Fuzzy Identity-based Cryptography.

Security level	Fuzzy Identity-Based Encryption (FIBE) (s)
Encryption - 80 bits	0.492
Decryption – 80 bits	1.892
Encryption - 192 bits	5.07
Decryption – 192 bits	21.296

Acknowledgments: 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, Reimann T, Alinier G. Cybersecurity for next generation healthcare in Qatar, Journal of Emergency Medicine, *Trauma & Acute Care* 2021 (2):41. http://dx.doi.org/jemtac.2021.qhc.41

[3] Okano H, Emura K, Ishibashi T, Ohigashi T, Suzuki T. Implementation of a strongly robust identity-based encryption scheme over type-3 pairings. *International Journal of Networking and Computing*, 2020;10:174–188.

[3] Sahai A, Waters B. Fuzzy identity-based encryption. In Annual international conference on the theory and applications of cryptographic techniques, 457–473. Springer, 2005.