CYBERSECURITY IN WIRELESS BODY AREA NETWORK (WBAN): PROPOSING A PRIVACY AND SECURITY FRAMEWORK FOR WEARABLE HEALTHCARE DEVICES AGAINST CYBER-ATTACKS

Nargiza Akramova
Westminster International University in Tashkent
Teacher at Department of Technology, Education and Law

Abstract:

Statement of the Problem: Having revolutionised the e-health technologies, the Wireless Body Area Networks (WBANs) has a great ability of collecting vital human body parameters through wearable sensors for further usage in various healthcare applications. WBANs have gained considerable attention of several health centres for making patient health monitoring processes easier and more affordable. These wearable devices are automatically measuring human blood pressure or insulin value and thus transmitting the data into hospitals. It is true that WBANs are contributing to improvement of health, however, the patient data before and after transmission out of the WBAN devices is subject to unauthorized access and manipulation. Thus, the security and privacy issues that come from WBANs usage in health monitoring is one of the major unresolved problems for the IoMT (Internet of Medical Things) researchers today and there is still a major gap for an integrated cyber protective framework to be specifically designed for all healthcare wearable devices of WBAN. This research focuses on fulfilling privacy and security requirements of WBAN users via proposing an integrated framework based on the results of primary and secondary research.

Methodology

The author has used a quantitative methodology tools surveying 72 respondents (primary research) and analysing the self-assessment questionnaire results of Department of Health Information Management, University of Pittsburgh of 31 e-health providers (secondary research). The research methodology was based on Positivism research philosophy and the researcher used Inductive research approach. Initially, for primary research questionnaires were given to sample population defined through Z-test technique. The results of the questionnaires helped the researcher to find out the cyber awareness and security preferences for wearable devices. This gave the author a general idea and focus areas for designing a security framework. Some of the notable findings of questionnaires are:

- Confidentiality is the top priority when using wearable devices for healthcare
- A huge number of users of wearable devices such as smart watches or fitness trackers have no idea how to act and whom to contact in case their wearables are compromised by attackers

- More than half of the respondents would sacrifice usability for the security of their wearable devices.

For secondary research, the researcher used a dataset belonging to the research team of Department of Health Information and Management, University of Pittsburgh. The researcher used descriptive analysis tools and aggregation methods to summarise the data to produce only relevant findings. The original research type of quantitative and used Yes/No/Not Given multiple choice statements surveying 31 IoMT providers in US (Zhou et al.,2019). Some notable findings from the secondary research are:

- Vendors believe that they can protect Personal Health Information (PHI) if the system uses cloud storage
- Several health centres and patients are not provided with any information about encryption details of the medical wearable devices used.
- Most of the IoMT devices still require reliable authorisation solutions.

Findings

Based on the results of the research, a new framework that would overcome privacy and security issues protecting sensitive data has been developed. The new framework integrates the most reliable security solutions for Encryption, Authorisation and Authentication and reveals 10 main security principles including cyber awareness solutions for all stakeholders of healthcare wearable devices. In addition to the solutions and security principles, the researcher introduces a new layered architecture for WBAN system, which is more straightforward and easier to follow compared to the previous architecture in the literature.

Conclusion & Significance

The five features that made this framework to be much more reliable than previously developed frameworks are:

1. The framework has designed a new layered architecture for wearable WBAN that is more straightforward and easier to use as a main guideline of Security professionals.
2. The framework adopted the latest reliable solutions including Cloud Based Storage, Encryption, Biomedical Authentication and Fog Based Access Control.
3. The framework covered the security for all components of WBAN including Wearable sensors, Coordinator device and Clinical Back-End Server.
4. The framework developed 10 principles based on the results of primary and secondary research.
5. The framework includes the cyber-awareness and incident response programs for the WBAN stakeholders.

References

1. Zhou, L., Thieret, R., Watzlaf, V., Fahima, R., Dealmeida, D. and Parmanto R.B. (2019). A Telehealth Privacy and Security Self-Assessment Questionnaire for Telehealth providers: Development and Validation. International Journal of Telerehabilitation, 11(1), pp. 3-14.