Risk Evaluation and Attack Detection in Heterogeneous IoMT devices using Hybrid Fuzzy Logic Analytical Approach

Abstract

The rapidly expanding Internet of Medical Things (IoMT) landscape fosters enormous opportunities for personalized healthcare, yet it also exposes patients and healthcare systems to diverse security threats. Heterogeneous IoMT devices present challenges that need comprehensive risk assessment due to their varying functionality, protocols, and vulnerabilities. Hence, to achieve the goal of having risk-free IoMT devices, the authors used a hybrid approach using fuzzy logic and the Fuzzy Analytical Hierarchy Process (FAHP) to evaluate risks, providing effective and useful results for developers and researchers. The presented approach specifies qualitative descriptors such as the frequency of occurrence, consequence severity, weight factor, and risk level. A case study with risk events in three different IoMT devices was carried out to illustrate the proposed method. We performed a Bluetooth Low Energy attack on an oximeter, smartwatch, and smart peak flow meter to discover their vulnerabilities. Using the FAHP method, we calculated fuzzy weights and risk levels, which helped us to prioritize criteria and alternatives in decision-making. Smartwatches were found to have a risk level of 8.57 for injection attacks, which is of extreme importance and needs immediate attention. Conversely, jamming attacks registered the lowest risk level of 1, with 9 being the maximum risk level and 1 the minimum. Based on this risk assessment, appropriate security measures can be implemented to address the severity of potential threats. The findings will assist healthcare industry decision-makers in evaluating the relative importance of risk factors, aiding informed decisions through weight comparison.