SECURE for Student Success

Undergraduate Research Program

Department of Computer Science

Research Duration:	Summer 2025 (June – August 2025)
Faculty:	Rashida Hasan
Email address:	rashida.hasan@csun.edu
Contact No:	Room: JD 4414, Phone: 3373261546
Title of Project:	Towards Secure Healthcare IoT Networks: Anomaly Detection Framework for Safeguarding Medical Devices and Patient Information

a. Overview and Rationale

The integration of Internet of Things (IoT) technology in healthcare has significantly improved patient monitoring, diagnostics, and overall healthcare delivery. In healthcare, IoT enables the use of wearable devices that continuously collect vital data from patients, including measurements such as oxygen levels, blood pressure, blood sugar, and heart rates. However, this increased reliance on interconnected medical devices poses significant security challenges, as cyber threats, unauthorized access, and data breaches can compromise sensitive patient information and endanger patient safety. This proposal seeks to develop a robust anomaly detection framework utilizing advanced machine learning algorithms to enhance the security of healthcare IoT networks. By identifying deviations from normal operational patterns in device behavior and network traffic, this framework aims to safeguard medical devices and ensure the confidentiality, integrity, and availability of patient data.

b. Goal:
The primary goal of this project is to develop and validate an advanced anomaly detection framework that effectively monitors and secures healthcare IoT networks. This framework will utilize machine learning algorithms to identify anomalous behaviors in medical devices and network traffic, ultimately safeguarding sensitive patient information and ensuring the uninterrupted operation of healthcare services

c. Objective
- To develop a comprehensive anomaly detection framework tailored specifically for healthcare IoT environments to effectively identify security threats.
- To improve the detection and response capabilities of medical devices against unauthorized access and potential breaches.
- To ensure the integrity and confidentiality of patient data through advanced monitoring and anomaly detection techniques.
- To validate the effectiveness of the framework in real-world healthcare scenarios through rigorous testing and performance evaluation.

d. Methodology
The proposed methodology consists of two modules:
i. Feature Selection module: This module involves acquiring data from various healthcare IoT devices, such as wearables and medical equipment. The collected data will be cleaned to remove inconsistencies and normalized to standardize values. Relevant features will then be extracted to capture key metrics related to device performance and patient health.
ii. Anomaly Detection Module: This module leverages the Isolation Forest algorithm to introduce a novel approach for detecting anomalies in healthcare IoT devices. By constructing multiple decision trees that isolate anomalies based on their unique path lengths, the framework will effectively distinguish between normal and anomalous behaviors in device data
iii. Dataset: We will use the publicly available dataset to evaluate the performance of our model.

e. Expected Outcomes
- A fully functional anomaly detection framework that significantly enhances the security of healthcare IoT networks.
- Students will deliver poster and oral presentations at the annual sfs^2 research symposium in early fall 2025, showcasing the outcomes of this research project.

f. Deliverables
- Final Research Report: A comprehensive report summarizing the research findings, framework development, and evaluation results
- Prototype Framework: A prototype of the anomaly detection framework, including source code and detailed implementation instructions.