Threat Detection in Remote Patient Health Monitoring Systems Using Machine Learning

Ankita Kudale
Department of Computer Engineering Alard College of Engineering & Management, Pune, India

Dipali Mane
Department of Computer Engineering Alard College of Engineering & Management, Pune, India

Abstract

Remote Patient Health Monitoring (RPHM) systems have gained significant importance in modern healthcare by enabling continuous monitoring of patients outside traditional clinical environments. However, the integration of IoT devices, cloud platforms, and communication networks introduces serious cybersecurity challenges. These systems are vulnerable to threats such as unauthorized access, data manipulation, and network- based attacks, which may compromise patient safety.

A hybrid dataset integrating physiological signals and net- work activity features is utilized to represent realistic health- care scenarios. Multiple classification models, including Logistic Regression, Support Vector Machine (SVM), Random Forest, and XGBoost, are trained and analyzed to identify abnormal system behavior. The dataset is systematically preprocessed to remove redundant correlations and to incorporate variability that reflects real-world operational conditions. This approach enables accurate and reliable detection of potential cyber threats in distributed healthcare systems.

Experimental results show that XGBoost achieves the highest detection performance, while Random Forest provides a balance between accuracy and interpretability. The proposed system improves the reliability and security of remote healthcare systems and demonstrates its applicability in real-world scenarios.

Index Terms

Remote Patient Monitoring, Threat Detection, Machine Learning, Cybersecurity, XGBoost, Random Forest, Healthcare IoT