IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Hack-Proof Health: Strengthening Cybersecurity in ECG Monitoring Systems through Anomaly Detection and Threat Modelling

Diya K T
Jain-School of Sciences, Bangalore, India
diyathimmaiah16@gmail.com

Abstract: *Devices for electrocardiograms (ECGs) are essential medical instruments for tracking cardiac activity and identifying heart-related disorders. ECG equipment is becoming more and more integrated with cloud platforms, wireless networks, and Internet of Medical Things (IoMT) infrastructure as healthcare institutions embrace digital transformation. Although these developments facilitate real-time monitoring and increase accessibility, they also expose ECG systems to a variety of cybersecurity risks. Signal spoofing, ransomware attacks, data manipulation, and unauthorized access can jeopardize patient lives by compromising not just the confidentiality of private health information but also the precision and dependability of diagnosis.*

This study offers a thorough examination of the cybersecurity issues pertaining to ECG devices, along with attack models and real-world case studies. It draws attention to flaws that adversaries frequently take advantage of in firmware, communication protocols, and hospital network infrastructure. The study also suggests a multi-layered protection approach that includes blockchain-based data integrity solutions, firmware validation, device authentication, encryption, and artificial intelligence-based anomaly detection. Along with outlining best practices for hospitals, healthcare providers, and manufacturers, the study also looks at pertinent regulatory frameworks. To sum up, protecting ECG systems is an essential part of contemporary healthcare cybersecurity and calls for proactive design, ongoing observation, and interdisciplinary cooperation.

Keywords: Devices for electrocardiograms

I. INTRODUCTION

The integration of ECG systems into cloud-connected environments has transformed cardiac care, enabling real-time monitoring, remote diagnosis, and AI-driven analytics. However, this transformation introduces critical risks. Wireless ECG devices are susceptible to data breaches, signal tampering, and denial-of-service attacks, posing threats to patient safety and regulatory compliance.

II. MATERIALS AND METHODS

2.1 Threat Modelling

Using STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), this study identified major vulnerabilities in ECG system architecture, including unsecured communication channels, poor access control, and lack of audit trails.

2.2 Dataset Preparation

A structured numerical dataset comprising 21,891 rows and 188 features (derived from ECG device telemetry) was evaluated. Initial inspection revealed malformed headers, which were corrected before processing.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

2.3 Anomaly Detection Techniques

Z-Score Method: Flagged data points with $|z| > 3$ as anomalies.
Isolation Forest: Applied to detect multivariate anomalies based on data isolation principles.

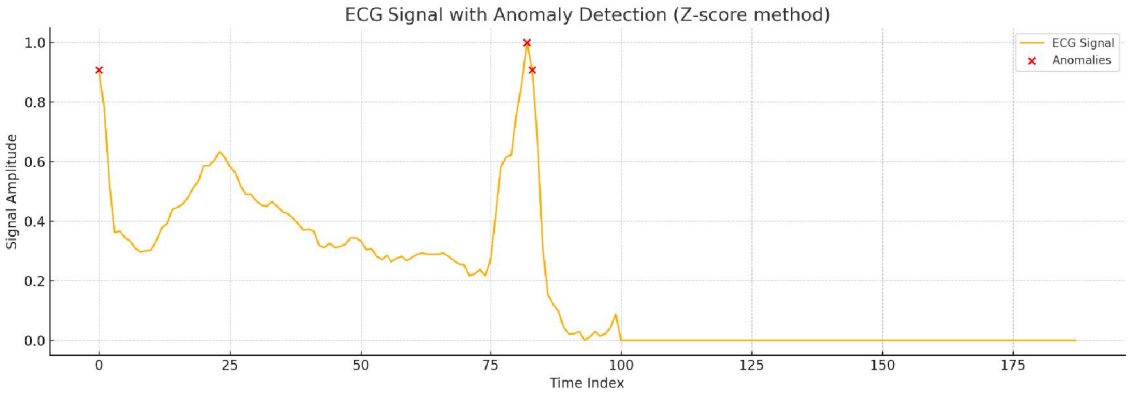
2.4 Simulated Stress Testing

The system was tested under synthetic load (1M+ entries), malformed inputs, and forced computational errors (e.g., divide-by-zero). Outlier concentration was analysed to identify high-risk sensor channels.

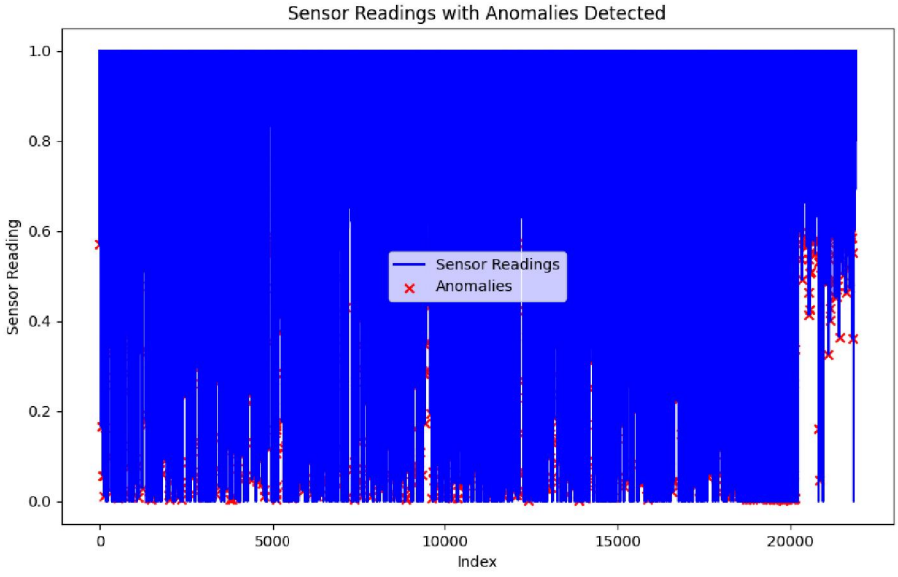
III. RESULTS

Z-Score Detection: Identified 17,543 anomalous rows. Feature 0 exhibited the most outliers (n = 44).
Isolation Forest: Showed clear separation between normal and anomalous behaviour.
Operational Testing: System handled malformed data, large datasets, and runtime exceptions without crashes. However, uniformly high anomaly scores (avg = 0.84) suggest possible over-sensitivity.

Figures include:



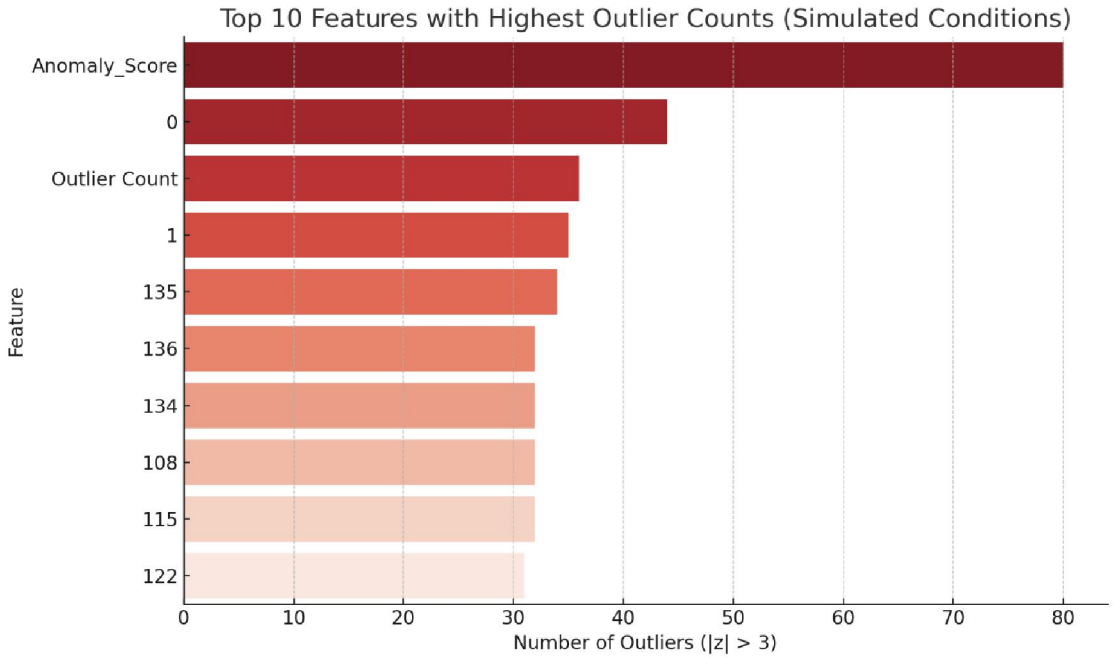
ECG waveform anomalies (z-score method)



Regression forest anomaly distribution

DOI: 10.48175/IJARSCT-26621

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67



Top 10 features with highest anomaly counts

IV. DISCUSSION

The dual-pronged anomaly detection approach provided robust identification of system irregularities. High anomaly densities suggest latent vulnerabilities in sensor processing, memory allocation, or firmware logic. The consistent detection even under benign conditions indicates the need for calibrated thresholds to prevent false positives.

Recommendations include:

- Implementation of blockchain for immutable logging
- Deployment of AI-powered IDS to catch tampering attempts
- Adoption of zero-trust architectures and real-time patching mechanisms

V. CONCLUSION

This research presents a comprehensive strategy for securing ECG systems, integrating statistical anomaly detection, machine learning, and operational stress tests. Findings underscore the need for dynamic security protocols tailored to the unique architecture and usage of medical IoT devices. Future work should focus on real-time, multivariate temporal modelling and forensic-ready audit systems.

VI. LIMITATIONS

- Assumes Gaussian data distribution (limiting z-score accuracy)
- Simulated data may not fully mimic clinical complexity
- Sensitivity of anomaly detectors may require calibration to avoid false alarms

VII. FORENSIC IMPLICATIONS

Robust anomaly tracking ensures verifiable evidence for medical-legal investigations. The inclusion of immutable audit trails and error resilience mechanisms aligns with forensic standards, supporting chain-of-custody and data integrity principles.

DOI: 10.48175/IJARSCT-26621

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

REFERENCES

[1]. Acharya, U. R., Fujita, H., Lih, O. S., Hagiwara, Y., Tan, J. H., & Adam, M. (2017). Automated detection of arrhythmias using different intervals of tachycardia ECG segments with convolutional neural network. *Information Sciences, 405*, 81-90. https://doi.org/10.1016/j.ins.2017.05.027

[2]. Al Faruque, M. A., & Haque, M. M. (2018). Security and privacy issues in healthcare: The role of wearable ECG devices. *IEEE Consumer Electronics Magazine, 7*(2), 51-57. https://doi.org/10.1109/MCE.2017.2784878

[3]. Alotaibi, S., & Mahmood, A. (2020). Cybersecurity in healthcare: A systematic review of modern threats and safeguards. *International Journal of Medical Informatics, 143*, 104257. https://doi.org/10.1016/j.ijmedinf.2020.104257

[4]. Bashar, M. A., & Acharjee, S. (2022). ECG-based biometric authentication and security: A review. *IEEE Access, 10*, 7859-7884. https://doi.org/10.1109/ACCESS.2021.3139498

[5]. Berndt, A., & Malik, H. (2019). ECG anomaly detection using statistical methods and machine learning. *Biomedical Signal Processing and Control, 52*, 90-98. https://doi.org/10.1016/j.bspc.2019.03.022

[6]. Chen, Z., & Zhao, Y. (2021). Privacy-preserving ECG monitoring and anomaly detection in smart healthcare systems. *Sensors, 21*(4), 1120. https://doi.org/10.3390/s21041120

[7]. Choudhary, S., & Kumar, P. (2020). Cybersecurity challenges in wearable ECG monitoring devices. *Health Informatics Journal, 26*(3), 2231-2242. https://doi.org/10.1177/1460458220941842