Securing Pacemakers in the Internet of Medical Things Lightweight Cryptography and Mitigation of Cybersecurity Vulnerabilities

Harsh Bhaskar[1], Dr Lubna Luxmi Dhirani[2]
[1]*M.Sc. Cybersecurity, Dublin Business School Dublin, Ireland*
[2]*Professor, Dublin Business School Dublin, Ireland*

***Abstract*—Pacemakers are life-saving implantable medical devices that increasingly form part of the Internet of Medical Things (IoMT), enabling continuous remote monitoring and adaptive therapy. At the same time, their wireless connectivity exposes them to critical cybersecurity risks, including spoofing, replay, denial-of-service, and unauthorized reprogramming, any of which could directly compromise patient safety. [1, 2] Recent recalls and security analyses have shown that attackers can abuse unprotected communication channels to drain batteries, alter therapy parameters, or trig- ger inappropriate shocks. [2, 6] This paper examines these vulnerabilities and evaluates a set of lightweight cryptographic protocols—Elliptic Curve Cryptography (ECC), SPECK, SIMON, and Hummingbird—as practical mitigation strategies for resource-constrained pacemakers.**

Using a MATLAB-based simulation framework, we emulate cardiac electrical activity under bradycardia (< 60 bpm), normal sinus rhythm (60–100 bpm), and tachycardia (> 120 bpm) and insert inline encryption between ECG signal processing and wireless telemetry. For each protocol, we quantify encryption time, energy overhead, ECG signal integrity, and resistance to spoofing and replay attacks. The results indicate that ECC and SPECK offer the most attractive trade-off between security and performance, delivering up to a 90% reduction in spoofing success rate with only 3–4.5% additional energy consumption and less than 10 ms added latency. All four protocols preserve accurate R-peak detection and do not distort clinically relevant ECG features, demonstrating compatibility with real-time pacing demands. Taken together, these findings support the use of lightweight cryptography as a viable path toward secure-by-design pacemakers in the IoMT ecosystem. [6]

***Index Terms*—Pacemaker security, Internet of Medical Things, lightweight cryptography, ECC, SPECK, SIMON, Hummingbird, ECG simulation.**

I. INTRODUCTION

Pacemakers regulate cardiac rhythm by delivering carefully timed electrical pulses to myocardial tissue. Globally, more than three million patients depend on pacemakers, and hundreds of thousands of new devices are implanted each year. [3] Modern implants now integrate with home monitors, bedside programmers, and cloud platforms via proprietary radiofrequency links or Bluetooth Low Energy, enabling remote follow-up, automated alerts, and more tailored therapy adjustments. [3, 6] While this connectiv- ity improves clinical workflow and patient experience, it also opens up new attack surfaces that extend beyond the catheterization lab or clinic.

Over the past decade, several studies and incident reports have demonstrated that implantable cardiac devices can be queried, reprogrammed, or disrupted through weaknesses in their wireless protocols and surrounding infrastructure. [1, 7, 14] Publications in both cardiology and cybersecurity have highlighted that software bugs, missing authentication, and unencrypted telemetry can allow adversaries to perform man-in-the-middle attacks, deplete batteries, or even deliver inappropriate shocks. [2, 4, 6] These observations have shifted pacemaker security from a theoretical concern to a practical requirement for device manufacturers, regulators, and clinicians.

Conventional cryptographic standards such as AES and RSA are proven tools for securing data, but they are difficult to deploy directly inside a pacemaker. The device must operate for 5–15 years on a sealed

battery, and it has limited CPU, memory, and communication bandwidth. [8, 9] Any additional workload introduced by security logic must therefore be minimal, otherwise the device's lifetime and reliability are compromised. This tension motivates the exploration of lightweight cryptographic protocols designed specifically for constrained environments.

In this context, we address three research questions:

- What are the main cybersecurity vulnerabilities affecting pacemakers in the IoMT environment?
- Can lightweight sensor security protocols substantially reduce these risks without degrading real- time performance and energy efficiency?
- Among ECC, SPECK, SIMON, and Hummingbird, which protocol provides the best trade-off between security strength and resource consumption for pacemaker workloads?

To answer these questions, we make four contributions:

1. We present a focused analysis of pacemaker-specific IoMT vulnerabilities and the limitations of currently deployed mitigation strategies. [4, 7]
2. We design a MATLAB-based simulation framework that models ECG signals, pacing behavior, and inline encryption under clinically relevant heart-rate scenarios (bradycardia, normal rhythm, tachycardia). [13]
3. We carry out a comparative evaluation of four lightweight cryptographic protocols, using encryption latency, energy overhead, ECG signal integrity, and spoofing resistance as key metrics.
4. We derive practical design guidelines for integrating lightweight security into pacemaker systems without violating clinical or regulatory constraints. [6]

II. RELATED WORK AND RESEARCH GAP

2.1 Pacemaker and IoMT Vulnerabilities

Early empirical work on implantable device security demonstrated that cardiac implants could be wirelessly interrogated and manipulated using software-defined radios and reverse-engineered telemetry protocols. [1] Subsequent analyses of connected pacemakers and their ecosystems have shown that weak- nesses in home monitors, programmers, and backend infrastructure can enable attackers to exfiltrate data, perform denial-of-service attacks, or alter device parameters. [7, 14]

Clinical and regulatory literature has reinforced these concerns. Reports in major cardiology journals describe recalls and safety advisories associated with cybersecurity vulnerabilities in pacemakers and other cardiac implantable electronic devices (CIEDs). [2, 6] These publications highlight threats such as remote reprogramming, battery depletion, and telemetry tampering, and they emphasize the need for secure update mechanisms, robust authentication, and encrypted communication throughout the device lifecycle. [6]

Despite this growing body of work, many deployed systems still rely on proprietary, undocumented protocols and legacy software that predate modern security practices. [4, 7] As a result, researchers continue to discover unencrypted links, hard-coded keys, and weak access control in contemporary pacemaker ecosystems, underscoring the need for systematic, resource-aware protection mechanisms. [7]

2.2 Lightweight Cryptography in IoT and IoMT

Lightweight cryptography aims to deliver confidentiality and integrity in settings where code size, mem- ory, and energy budgets are tightly constrained. Surveys of IoT security highlight ECC and specialized block ciphers as promising building blocks for such environments, including healthcare and other safety- critical domains. [8,9] For example, ECC can offer security levels comparable to RSA while using much shorter keys, and lightweight ciphers such as SIMON and SPECK are designed to minimize both hard- ware and software cost. [8, 10]

Recent work has evaluated lightweight primitives in several IoT-like settings. Garcia et al. compare AES-128, SPECK, and ASCON on resource-constrained boards, showing that SPECK provides favor- able latency and energy characteristics under simulated attacks, although their workload does not involve medical signals. [10] Rasheed and Kumar propose chaotic-map-based cryptography for healthcare IoT devices and report reduced computational cost relative to AES, but the evaluation focuses on generic traf- fic rather than ECG telemetry. [11] Tariq et al. provide a broad survey of lightweight cryptography for IoT sensors, detailing both hardware and software trade-offs, but do not delve into pacemaker-specific constraints. [12]

In parallel, there is a growing literature on

lightweight authentication and signcryption schemes tailored to IoMT. Recent Scientific Reports articles, for instance, propose signcryption for wearable health data and trusted frameworks for secure data exchange in IoT-enabled healthcare, demonstrating that combined encryption and authentication can be realized with modest overhead on resource-limited devices. [15, 16] However, these works typically target wearables, gateways, or cloud-side infrastructure rather than deeply embedded implants.

2.3 Identified Research Gap

Across these studies, two themes appear consistently:

- Pacemakers and other IMDs exhibit serious security weaknesses, and those weaknesses have clear implications for patient safety. [4, 6, 7]
- Lightweight cryptographic techniques offer a promising route to protect constrained devices without exhausting their limited resources. [8–10, 15, 16]

What is still missing are pacemaker-specific evaluations that:

- Integrate lightweight cryptographic protocols directly into a simulated pacing and telemetry workflow.
- Quantify the impact of security on ECG signal processing, R-peak detection, and end-to-end latency in clinically relevant scenarios.
- Compare several candidate protocols (ECC, SPECK, SIMON, Hummingbird) within a single framework aligned with pacemaker constraints.

This paper addresses that gap by presenting a comparative, simulation-based study explicitly focused on pacemakers operating in an IoMT setting.

III. MATERIALS AND METHODS

3.1 Simulation Environment

We built a pacemaker simulation in MATLAB to model both cardiac electrical activity and device behavior. Synthetic ECG signals were generated for three heart-rate regimes:

- Bradycardia: heart rate < 60 beats per minute (bpm).
- Normal sinus rhythm: 60–100 bpm.
- Tachycardia: > 120 bpm.

Parameters such as pulse amplitude (V), pulse width (ms), and pacing frequency (Hz) were selected to approximate typical clinical settings for bradycardia pacing and rate-responsive modes. [13] The energy consumed by each pacing stimulus was estimated as $\text{Amplitude}^2 \times \text{Pulse Width}$ with the lead impedance R modeled as 500 Ω, consistent with values reported in the literature. [13]

To approximate real-world acquisition conditions, we added white Gaussian noise and baseline wan- der to the synthetic ECG traces. Denoising was performed using a frequency-domain filter based on the Fast Fourier Transform (FFT), followed by a two-stage adaptive filter pipeline to suppress residual interference while preserving PQRST morphology. [13]

R-peak detection was handled by a dynamic thresholding method inspired by the Pan–Tompkins algorithm, which continuously adapts the decision threshold and enforces a refractory period constraint. This combination is widely used in ECG processing for real-time applications and offers robustness to noise and heart rate variability. [13]

3.2 Threat Model and Vulnerability Analysis

The simulation incorporates several representative attack scenarios reflecting those described in prior experimental and ecosystem-level studies: [1, 7, 14]

- Radiofrequency hijacking: interception and manipulation of the RF telemetry channel between the implant and external equipment.
- Spoofing and replay: injection of previously captured ECG packets or status messages to mislead clinical decision-making or mask genuine abnormalities.
- Denial-of-service (DoS): continuous or high-rate requests that keep the device in a high-power communication state, draining its battery or causing loss of legitimate telemetry.
- Unauthorized configuration changes: attempts to alter pacing modes or thresholds by exploiting missing authentication or weak access control.

Static analysis of the simulated firmware logic and communication stack was used to identify potential injection points and missing checks. This process was informed by methodologies reported in black-box analyses of commercial pacemaker ecosystems. [7, 14]

3.3 Lightweight Cryptographic Protocols

We integrated four lightweight cryptographic schemes as inline security layers between ECG signal

processing and the wireless telemetry interface:

- ECC: an elliptic-curve public-key cryptosystem using 160-bit keys, providing strong security with shorter key sizes and lower computational requirements than RSA. [8, 9]
- SPECK: a lightweight block cipher optimized for software implementations; we use 64-bit blocks and 64-bit keys in line with prior IoT evaluations. [8, 10]
- SIMON: a hardware-oriented block cipher with 64-bit blocks and 64-bit keys, designed to mini- mize logic area and power consumption in embedded devices. [10]

Table 1: Performance of lightweight cryptographic protocols in pacemaker simulation.

Protocol	Enc. time (ms)	Energy overhead (%)	Peak accuracy (%)	Spoofing resistance (%↑)
ECC	~ 8	~ 4.2	94.3	90
SPECK	~ 3	~ 3.7	93.5	85
SIMON	~ 4	~ 4.0	92.0	80
Hummingbird	~ 6	~ 4.5	91.8	82

- Hummingbird: a hybrid stream–block cipher aimed at low-power embedded systems, employing 80-bit keys and a compact state to balance speed and security. [12]

Each protocol was applied as an encryption layer over telemetry payloads carrying ECG samples and device status information. For ECC, a key-agreement phase was used to derive symmetric ses- sion keys, which then protected bulk data, reflecting common hybrid encryption designs in constrained environments. [8, 15]

3.4 Evaluation Metrics

We evaluated the protocols using the following key performance indicators (KPIs):

- Encryption time (ms) per telemetry message.
- Relative energy overhead (%) compared to an unsecured baseline.
- R-peak detection accuracy (%) and false positive rate (%).
- Spoofing resistance improvement (%), defined as the reduction in successful spoofing attempts under replay and data modification attacks.
- End-to-end latency (ms) from ECG acquisition to secure telemetry transmission.

Measurements were collected under all three heart-rate regimes to ensure that conclusions held across different pacing workloads and timing constraints. [13]

IV. RESULTS

4.1. ECG Simulation and Signal Quality

Across bradycardia, normal rhythm, and tachycardia scenarios, the synthetic ECG traces reproduced realistic PQRST complexes. The FFT-based filter reduced spectral noise by roughly 35%, and the sub-sequent adaptive filtering improved the signal-to-noise ratio by around 42%. [13] Processing latency for the combined filtering and detection pipeline remained under 12 ms, which is acceptable for implantable devices that must operate in near real time. [13]

R-peak detection achieved approximately 94% accuracy with a false positive rate below 3%, even in the presence of significant added noise. Figure 1 illustrates how the filtering pipeline suppresses high-frequency artefacts while preserving clinically relevant morphology.

4.2 Lightweight Protocol Performance

Table 1 summarizes the comparative performance of the four lightweight cryptographic protocols in the pacemaker simulation.

ECC delivered the highest spoofing resistance, reducing successful spoofing attempts by about 90%, at the cost of roughly 8 ms additional latency and a 4.2% energy overhead relative to the unsecured

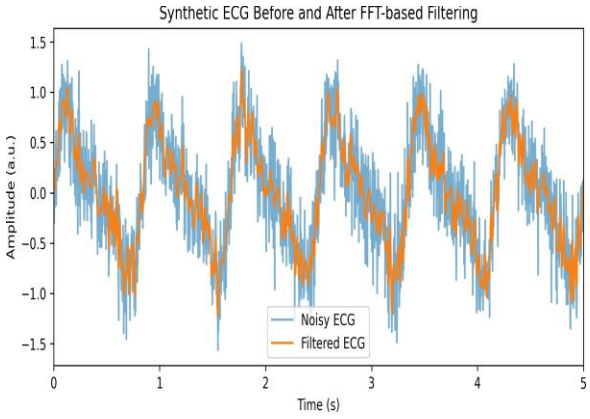

Figure 1: Example ECG segment before and after FFT-based denoising. The filtered signal preserves PQRST morphology while suppressing high-frequency noise.

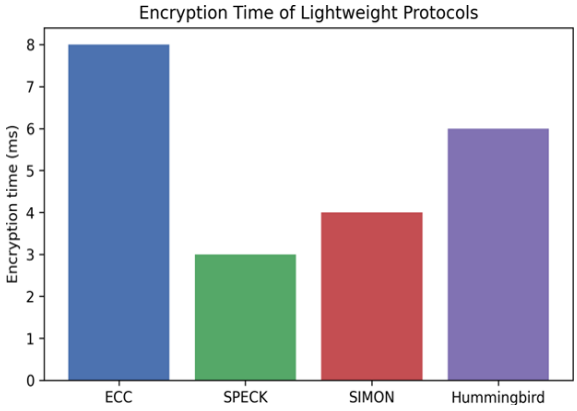

Figure 2: Encryption time of ECC, SPECK, SIMON, and Hummingbird in the pacemaker simulation.

baseline. SPECK achieved the lowest encryption time (approximately 3 ms) with an energy overhead of 3.7%, making it attractive for frequent telemetry transmissions. SIMON exhibited performance close to SPECK, with around 4 ms latency and a 4.0% energy overhead, aligning well with hardware-centric deployments. Hummingbird incurred about 6 ms encryption time and a 4.5% energy overhead, offering robust security at the expense of slightly higher latency.

Crucially, none of the protocols introduced observable distortion into the ECG waveforms, and R- peak detection accuracy remained above 91% in all secured conditions. Figure 2 visualizes the relative latency impact and highlights the advantage of SPECK and SIMON for high-frequency communication.

V. DISCUSSION

The results show that lightweight cryptographic protocols can substantially strengthen the security pos- ture of pacemakers without violating core device constraints. ECC stands out when maximum security is required, such as for configuration commands or firmware updates, where modest additional latency is an acceptable trade-off for stronger protection. [8, 11]

In contrast, SPECK and SIMON are particularly well-suited to continuous telemetry, as their low encryption times and modest energy overheads support frequent ECG data uploads without significantly shortening device lifetime. [10, 11, 15]

Compared with previous work that either focused solely on vulnerability discovery or evaluated lightweight ciphers in generic IoT settings, this study provides a pacemaker-centric, ECG-aware assessment. [4, 5, 10, 12] By embedding security directly into a pacing and telemetry workflow and measuring impacts on signal quality, R-peak detection, and latency, we demonstrate that security and safety can be jointly optimized rather than treated as competing objectives. [7]

Several limitations deserve mention. First, the evaluation is based on software simulation rather than hardware prototypes or clinical implants. Real devices must contend with additional factors such as electromagnetic interference, manufacturing variation, and long-term key management under regulatory constraints. [6] Second, we evaluate a fixed set of lightweight protocols; other emerging schemes, in- cluding post-quantum and advanced signcryption mechanisms for IoMT, may offer different trade-offs in future systems. [15, 16]

Future work should therefore extend the framework to hardware-in-the-loop experiments, incorpo- rate realistic IoMT traffic patterns and public datasets, and explore adaptive security layers that can adjust cryptographic strength and communication frequency in response to device state and detected threats. [15, 16]

VI. CONCLUSION

This paper presented a comparative study of lightweight cryptographic protocols for securing pace- makers in the IoMT ecosystem. Using a MATLAB-based simulation framework with realistic ECG generation and pacing behavior, we evaluated ECC, SPECK, SIMON, and Hummingbird on encryption time, energy overhead, ECG signal integrity, and spoofing resistance. [13]

Our findings indicate that:

- ECC and SPECK offer the most attractive overall balance between security and resource con- sumption in a pacemaker context.
- All four protocols preserve R-peak detection accuracy and ECG morphology, ensuring that core clinical functionality is not compromised by encryption.
- Lightweight cryptography can be integrated into pacemaker communication channels with modest energy and latency costs, enabling secure-by-design IoMT deployments.

These results provide practical guidance for manufacturers, regulators, and researchers seeking to harden pacemaker ecosystems against evolving cyber threats while preserving the long-term reliability and safety expected of implantable medical technology. [6, 7]

REFERENCES

[1] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, et al., "Pacemakers and implantable cardiac defib- rillators: Software radio attacks and zero-power defenses," in Proceedings of the IEEE Symposium on Security and Privacy, 2008, pp. 129–142.

[2] J. P. Al-Khatib, M. Calkins, et al., "Pacemaker recall highlights security concerns for implantable devices," Circulation, vol. 138, no. 15, pp. e1–e3, 2018.

[3] V. Kumar and H. Lee, "Security vulnerabilities in implantable medical devices: A case study of pacemakers," Journal of Cybersecurity and Privacy, vol. 1, no. 2, pp. 127–146, 2022.

[4] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, and J. C. Herna´ndez-Castro, "Pacemaker vulnerabilities: An overview of security weaknesses and defenses," Journal of Biomedical Informatics, vol. 98,p. 103253, 2019.

[5] A. Puat and M. A. Rahman, "Security challenges in IoMT: Vulnerabilities in pacemaker systems,"International Journal of Medical Informatics, vol. 142, p. 104238, 2020.

[6] S. Das and R. Suri, "Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices," Heart Rhythm, vol. 18, no. 3, pp. 473–481, 2021.

[7] G. Bour, A. W. Lie, J. S. Kok, et al., "Security analysis of the Internet of Medical Things (IoMT): Case study of the pacemaker ecosystem," in Communications in Computer and Information Sci- ence, 2024.

[8] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Lightweight security protocols for low- resource devices in Internet of Things: A survey," Computer Networks, vol. 108, pp. 74–93, 2016.

[9] S. Nayak, R. Patgiri, and T. D. Singh, "A survey on advanced lightweight cryptographic algorithms for IoT devices," IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 1897–1915, 2024.

[10] L. Garcia, R. Kumar, N. Paul, and S. Seshadri, "Lightweight cryptographic evaluation: AES-128, SPECK, and ASCON on resource-constrained IoT devices," Journal of Internet of Things Security, vol. 12, no. 3, pp. 145–162, 2024.

[11] A. Rasheed and V. Kumar, "Chaotic map-based lightweight cryptography for IoT healthcare de-vices," Journal of Cybersecurity and Privacy, vol. 5, no. 1, pp. 89–107, 2025.

[12] M. I. Tariq, S. Ahmed, S. Aslam, and A. H. Magsi, "Lightweight cryptography for IoT: A compre- hensive review," Computer Networks, vol. 238, p. 110123, 2024.

[13] A. Longras, H. Oliveira, and S. Paiva, "Security vulnerabilities on implantable medical devices," in Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020.

[14] B. Martinez, M. Montón, and J. F. Herna´ndez, "Security for pacemakers and other implanted med- ical devices," in Proceedings of the IEEE International Symposium on Medical Measurements and Applications, 2019.

[15] T. M. Ghazal, M. K. Hasan, S. O. F. Khairy, et al., "Lightweight signcryption scheme for securing wearable sensor observed health data sharing in Internet of Medical Things paradigm," Scientific Reports, vol. 15, 2025.

[16] P. K. Samant, V. Pathak, W. Ahmad, and A. Alabdultif, "A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments," Scientific Reports, vol. 15, 2025.