Securing the Next-Generation Digital Lifeline: Firmware Integrity, Supply Chain Security, and Penetration Testing in Medical Devices

RAJAPAKSHA R. M. P .U
Sri Lanka Institute of Information Technology
BSc (Hons) in Information Technology - Cyber Security Specialization
Email: it23265592@my.sliit.lk

***Abstract* -** Wearable monitors, infusion pumps, and implantable sensors form a fast-growing group of networked medical devices. The platforms rely increasingly on advanced firmware, third-party libraries, and wireless updates. Although connectivity improves clinical functionality, it adds to the cyberattack surface across the entire device lifecycle ; design and manufacturing, deployment, and extended support.

This evaluation is focused on three major areas: (i) firmware integrity controls such as secure/verified boot, hardware roots of trust, authenticated updates, rollback protection, and runtime defenses; (ii) software supply chain security, such as SBOM generation, dependency management, vulnerability disclosure, and use of the Vulnerability Exploitability eXchange (VEX); and (iii) penetration testing approaches which must balance demanding security testing and cautious safety constraints.

Today's frameworks like FDA premarket guidance, IMDRF principles, and standards such as IEC 62304, IEC 81001-5-1, NIST SP 800-193, UL 2900-2-1, and AAMI technical reports have refined security-by-design practices. But challenges persist: partial SBOMs, insufficient vulnerability assessment, fragile update mechanisms in legacy devices, and absence of standardized, reproducible penetration testing methodologies. It argues for the development of assurance cases that integrate threat models, test evidence, and ongoing SBOM-driven risk monitoring. By integrating early hardening approaches and continuous risk management, the medical device ecosystem can improve patient safety, regulatory trust, and device resilience through the depreciation of time.

***Index Terms* -** Medical devices, IoMT, firmware integrity, secure boot, SBOM, VEX, supply chain security, penetration testing, FDA, IMDRF, IEC 62304, IEC 81001-5-1, NIST SP 800-193, UL 2900-2-1, AAMI TIRs.

I. INTRODUCTION

In recent years, incidents have highlighted the threat posed by networked health devices' cybersecurity threats. In 2019, for example, the U.S. Food and Drug Administration (FDA) confirmed vulnerabilities in Medtronic pacemakers that would allow hackers to remotely alter device programming, potentially at risk of causing patients' lives to be endangered. Johnson & Johnson issued recalls of certain insulin pumps after testing demonstrated that the pumps can be wirelessly manipulated into delivering unauthorized doses. These illustrations indicate that security vulnerabilities in medical devices are not theoretical. They have real, direct impacts on patient safety.

Present-day healthcare increasingly depends on networked and computerized technology, including ventilators, pacemakers, infusion pumps, and portable monitors [2], [16]. Security weaknesses like ransomware, firmware tampering, or supply chain attacks may impede therapy, compromise device functionality, or penetrate sensitive healthcare information, ultimately endangering both patient safety and clinical functionality [1], [2], [9]. Threats such as URGENT/11 and Ripple20 also underscore that weaknesses in widely utilized communications libraries will spread to secure-critical systems [2], primarily due to contemporary devices relying on layered firmware and third-party code components [2], [5].

These risks affect an expansive set of stakeholders: patients, who rely on safe and effective treatment; healthcare professionals, who apply and manage these devices; manufacturers, who are accountable for secure design and maintenance; and regulators, who ensure compliance with compliance and safety protocols. In turn, industry standards and regulators increasingly call for robust firmware integrity controls, improved supply chain defenses, safety-focused penetration testing, and continuous postmarket surveillance [5], [6]. This review is focused on these three pillars, interlacing the best practices of today, regulation, and ongoing research challenges together to maintain a more robust and more reliable medical device environment.

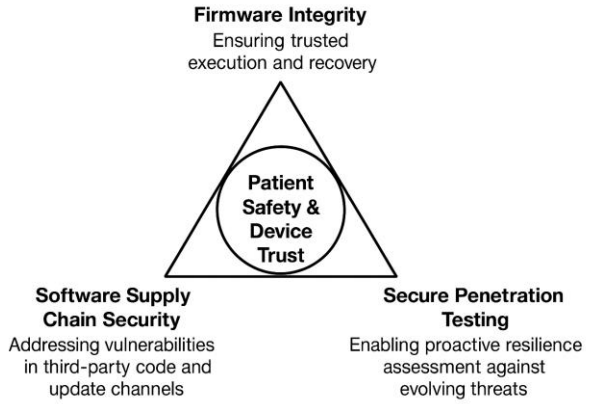


Fig. 1. The three interdepenndent pillars of next-generation medical device security

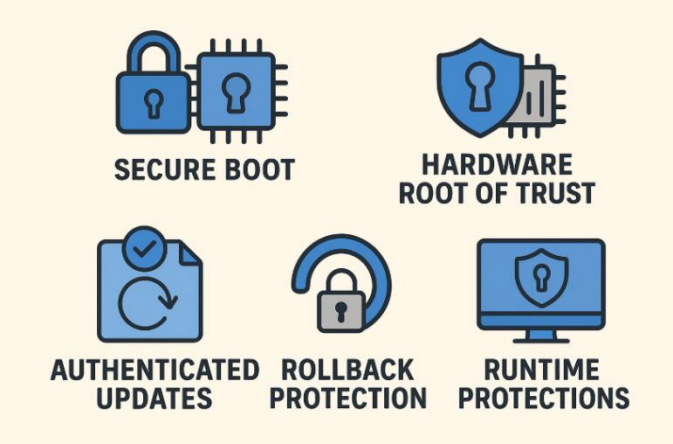
II. Research Statement and Objectives

All the literature, regulations, and standards related to (1)firmware integrity measures for medical devices, (2) software supply chain risk management, e.g., SBOM generation and vulnerability disclosure, and (3) penetration testing practices deployable in safety-critical healthcare settings are all carefully reviewed in this paper [5], [6], [2]. The objective is to combine best practices, identify gaps, and propose future research directions and an evidence based assurance strategy that meets legal requirements [5], [6].

III. Literature Review

Firmware Integrity in Safety-Critical Devices

Safe firmware is the foundation for safe device operation and reliability [5], [6]. Standard mechanisms are:



• *Secure/Verified Boot & Measured Boot:*

By checking the digital signatures on the bootloaders and firmware images and measuring pieces into a hardware-imposed trust store to verify, you can discover device trust at power on [5], [6]. Hardware roots of trust, anti-rollback indicators, partitioned recovery images, and design update logs are all used in actual implementations [5]. Medical device submissions are becoming more likely to include these mechanisms, which are consistent with platform firmware resiliency guidelines [5], [6].

- *Authenticated Update & Anti Rollback :*

Protected integrity, authenticated updates and version controls avoid downgrade attacks and untrusted payloads [5]. A/B partitioning, signed delta packages, and emergency recovery are some resilient update structures that reduce downtime [5].

- *Key Manufacturing & Management Trust :*

Cloning and unwanted changes are prevented by chain of trust establishment during manufacturing (one-time device keys, per component signing keys, certificate hierarchies and all) [5], [6]. Insider and supply chain attacks are reduced by securing signing infrastructure and enforcing least privilege within the build system [5].

- *Runtime Object Protections:*

When the runtime is compromised by an attacker, exploitability is reduced through control flow integrity, memory security hardening, least privilege allocation, and secure debug connections [3], [7].

Recent literature (2022 - 2024) highlights that IoMT medical devices are increasingly vulnerable to firmware tampering, with proof-of-concept exploits of attackers bypassing insecure bootloaders and unsigned updates [18], [19]. Studies have proposed hybrid models combining NIST SP 800-193 recommendations with IEC 60601 safety standards to address patient-critical firmware resilience [20]. Adoption, however, remains patchy among manufacturers, particularly in legacy infusion pumps and imaging devices where retrofitting secure boot is technically not feasible [21].

Synthesis :

NIST SP 800 193 forms the technical foundation of platform firmware resilience, according to available literature and guidance [5], [6]. The FDA initial guidance and IMDRF principles involve security by design expectations across the life cycle [5], [6]. Process structure for design inputs, verification, and maintenance is provided through integration with IEC 62304 (software life cycle) and IEC 81001 5 1 (health software security activities) [5], [6]. AAMI technical reports and UL 2900 2 1 convert these ideas to measurable test results [5].

Nonetheless, latest studies confirm that medical-specific firmware resilience models remain immature, especially in terms of safety trade-offs within recovery procedures and battery-powered implant limitations [18], [20]. Inadequacy reflects the need for industry-specific firmware assurance frameworks that connect resilience and clinical safety outcomes.

Software Supply Chain Risks and SBOM Practice

Third-party and open source components are also commonly employed in medical device software [2]. Their extremely common use in stacks can compromise medical devices years after their initial release, as illustrated in recent systemic weaknesses [2]. Strong supply chain management depends on:

- *SBOM Production and Quality*.

Generating machine readable SBOMs (eg: CycloneDX or SPDX) by build, showing versions and transitive dependencies, and complying with the minimum elements guidelines [5]. Completeness checks, vulnerability assessment, and component identification (PURL/CPE) are some quality practices [5].

- *SBOM Consumption and VEX.*

Reducing healthcare providers' false positives by operationally leveraging SBOMs for prioritizing newly discovered CVEs and disseminating VEX statements to signal exploitability in device contexts [5].

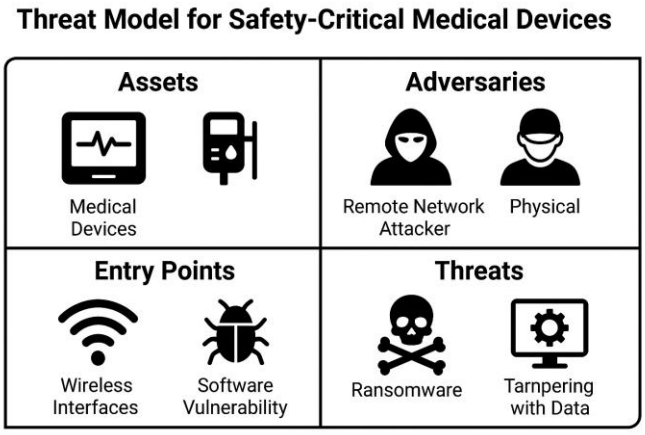
- *System and Artifact Integrity :*

The pipeline is protected against tampering by code signing, isolated and attested CI/CD, homogenized versions, in-toto

style provenance attestations, and developer identity protections [4], [10], [17].

- Coordinated Vulnerability Disclosure (CVD): Healthcare can respond promptly and easily because of formal intake and remediation processes with patient safety accounting timelines [5], [6].

Recent journal articles emphasize that uptake of healthcare SBOM is still unbalanced: while the U.S. FDA 2023 draft guidance essentially mandates SBOM for premarket submissions, European manufacturers' surveys report only 35% automated SBOM pipelines. Studies also show that partial SBOMs ; typically missing transitive dependencies ; diminish their value to hospital security teams. Furthermore, operationalization of VEX remains low, causing alert fatigue to clinical security teams.



Synthesis:

SBOM and coordinated disclosure have increasingly been deemed mandatory submission documents, rather than voluntary appendices, in industry guidance (FDA premarket, IMDRF, HSCC Joint Security Plan) [5], [6]. Tooling compatibility continues to be a problem in regulated environments, VEX adoption remains in infancy stages, and SBOM quality is a mixed bag [5].

Recent evidence is focused on the policy practice gap: while regulators encourage use of SBOM, clinical adoption is impaired by tool fragmentation, lack of integration into asset management within hospitals, and unresolved issues of liability when vulnerabilities have been made public. This gap calls for investigation into scalable SBOM validation frameworks and healthcare-focused VEX distribution models.

Summary Table :

Framework / Standard	**Focus Area**	**Strengths**	**Limitations / Gaps**
NIST SP 800-193 (Platform Firmware Resiliency)	Firmware integrity and recovery	Provides strong baseline for firmware validation and rollback protection	Limited guidance on medical-specific safety-critical constraints
FDA Premarket Cybersecurity Guidance (2023 Draft)	Risk management for medical devices	Encourages SBOM, secure updates, vulnerability disclosure	Non-binding, enforcement relies on manufacturers
IEC 62304 (Medical Device Software Lifecycle)	Software development process	Ensures structured lifecycle for safety-critical systems	Lacks explicit security testing focus
IMDRF Principles for Cybersecurity in Medical Devices	Global harmonization	Cross-national recommendations; lifecycle emphasis	High-level, lacks concrete implementation details
UL 2900 Series (Software Cybersecurit	Testing and certification	Provides penetration testing and vulnerability	Adoption limited in medical device sector

Framework / Standard	Focus Area	Strengths	Limitations / Gaps
y for Network-Connect le Products)		assessment benchmarks	

Penetration Testing for Medical Devices

In the healthcare industry, penetration testing must create security evidence without compromising patients details or breaking rules [5], [6]. Most important actions are:

- *Risk Informed Scoping:*

Map test goals onto safety critical assets and abuse cases based (eg: unauthorized alteration of therapy, tampering with telemetry) on risk analyses and threat models [5].

- *Method Selection:*

Although adhering to health care security controls and, as appropriate, utilizing representative laboratory facilities and simulation, combine static/dynamic analysis, protocol activation (wired/wireless), interface abuse(debug/UART/JTAG), update mechanism testing, and privilege escalation tests [3], [5], [8].

- *Aligned Standard Evidence :*

AAMI reports offer risk management alignment; FDA premarket guidance foresees security test objects and traceability to design inputs; UL 2900 2 1 mandates systematic testing (including fuzzing) of medical devices [5].

- Legacy Fleet and Clinical Integration :

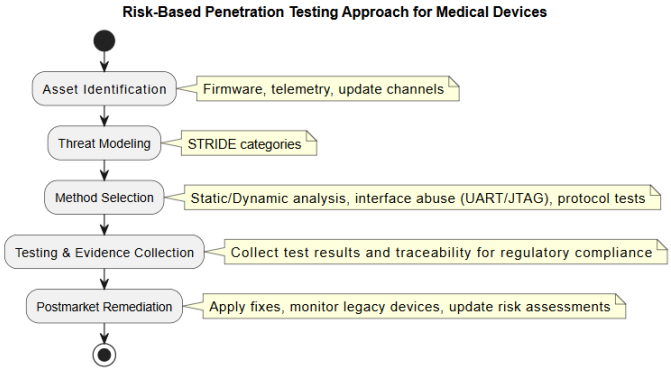
Medical Integration with the Legacy Fleet. Traditional devices, compensating controls in hospital networks, and provider coordination for remediation of vulnerabilities must all be considered in postmarket risk management [5], [6].

Recent penetration testing research has revealed that normal IoMT devices (pacemakers, insulin pumps, CT scanners, etc.) remain vulnerable to wireless protocol abuse and unsafe firmware updates despite IEC 62304 protocols compliance. The most significant reported difficulty lies in the absence of representative testbeds mimicking hospital environments without compromising patients' lives, thereby to under-tested cases in hospital networks. Scholarship also indicates that ethical/legal constraints; HIPAA in the United States and GDPR in the EU; restrict direct penetration testing on live systems, prompting simulation-based and "digital twin" approaches.

Synthesis :

The state of practice offers a significant value on identifiable evidence packages appropriate for regulatory analysis, reproducible lab setups, and whole, safety-minded testing related to risk assessment [5].

Despite this, there are gaps in harmonizing penetration testing approaches for IoMT devices regionally, in achieving cooperation between hospitals and vendors during testing, and in reconciling in-depth security testing and assurance with not disrupting patient care. These weaknesses necessitate harmonized frameworks that incorporate penetration testing into premarket certification and postmarket surveillance regimes.



IV. Future Research

The evolving threat landscape indicates that firmware, supply chain, and penetration testing security will require multi-disciplinary research in cybersecurity, medical engineering, and regulatory policy. The future research can be focused on the following:

Lightweight Cryptographic Mechanisms - Developing low power and resource-aware cryptography for wearable and implantable medical devices to provide improved firmware security without affecting device functionality.

Next-Generation Secure Update Mechanisms - Research into fault-tolerant over-the-air update mechanisms capable of managing partial connectivity, with robust authentication, rollback protection, and real-time patch verification.

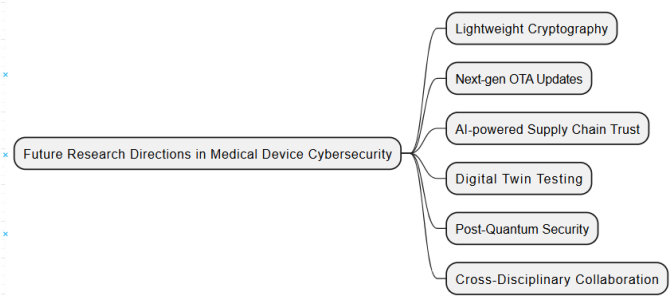
AI-Powered Supply Chain Trust - Utilizing machine learning and blockchain to detect anomalies in third-party libraries, predict supply chain vulnerabilities, and enforce compliance through real-time integrity monitoring systems [17].

Unified Testing Standards - Creating global penetration testing standards that ensure reproducibility across a range of medical devices, from wearable monitors and infusion pumps to implantable. The standards need to include risk-based test cases with patient safety as an inviolable constraint.

Integration of Digital Twins - Future penetration testing can incorporate digital twin technology, offering realistic, virtual replicas of medical devices to model cyber-physical attacks without exposing patients to danger.

Post-Quantum Security Considerations - Because medical devices are likely to be in service for many decades, researchers must look to the future arrival of quantum computing and investigate post-quantum cryptographic algorithms for long-term firmware resilience.

Cross-Disciplinary Collaboration - Tighter integration between cybersecurity professionals, biomedical engineers, and policymakers is the way forward to bridge the gap between regulatory compliance and actual security deployment in the healthcare sector.



V. Conclusion

Three keystones of cybersecurity for future generation medical devices are firmware integrity, software supply chain assurance, and safe penetration testing [5], [2]. Firmware integrity guarantees the device software remains unaltered and authentic and is therefore immune to harmful modification that may compromise patient safety [5]. Software supply chain assurance is concerned with the rigid management of third-party components, libraries, and updates with maximum disclosure in the shape of Software Bills of Materials (SBOMs) and Vulnerability Exploitability eXchange (VEX) practices to mitigate threats posed by external dependencies [5]. Secure penetration testing, however, is crucial in advance detection of vulnerabilities in devices, networks, and systems such that they cannot be weaponized [3], [7], [8], [13], [14], [15].

Regulatory and standards bodies such as FDA, IMDRF, NIST, IEC, UL, and AAMI recently published new guidelines that provide well organized templates to implement these cybersecurity practices [5], [6]. However, several important issues are still available. Test procedures are often not reproducible and standardized, which prevents results comparison among devices or institutions [5], [3]. Legacy

medical devices tend to have inadequate security and recovery processes, and thus become vulnerable to attack even when they are integrated into clinical workflows [5], [2]. Furthermore, global adoption of high quality SBOMs and VEX processes has not yet reached completion, resulting in inadequate visibility and accountability in the software supply chain [5].

In order to best safeguard patients and maintain digital trust for healthcare, medical device engineering must align with such guidelines while considering the practical limitations of existing systems [5], [6]. Such alignment requires not only the implementation of robust cybersecurity measures, but also the design of auditable artifacts that provide evidence of compliance, risk mitigation, and continuing surveillance [4], [5]. By doing so, health care organizations are able to demonstrate accountability, enable reproducible security validation, and establish trust among regulators, clinicians, and patients that health care devices are secure, reliable, and resilient in the more interconnected and digitally dependent world [5], [11], [16], [17].

VI. Appendix

- IoMT - Internet of Medical Things
- SBOM - Software Bill of Materials
- VEX - Vulnerability Exploitability eXchange
- CVD - Coordinated Vulnerability Disclosure
- FDA - U.S. Food and Drug Administration
- IMDRF - International Medical Device Regulators Forum
- IEC 62304 - Medical device software life cycle processes
- IEC 81001-5-1 - Health software and health IT security activities
- NIST SP 800-193 - Platform Firmware Resiliency
- UL 2900-2-1 - Cybersecurity for network-connectable products Healthcare
- AAMI TIRs - Association for the Advancement of Medical Instrumentation Technical Information Reports
- CFI - Control-Flow Integrity
- ASLR - Address Space Layout Randomization
- UART - Universal Asynchronous
- Receiver/Transmitter
- JTAG - Joint Test Action Group (debug interface)
- OTA - Over-the-air (updates)
- TPM - Trusted Platform Module
- RoT - Root of Trust
- PKI - Public Key Infrastructure
- CI/CD - Continuous Integration/Continuous Delivery
- PURL - Package URL
- CPE - Common Platform Enumeration
- CVE - Common Vulnerabilities and Exposures
- CWE - Common Weakness Enumeration
- CVSS - Common Vulnerability Scoring System
- SCA - Software Composition Analysis
- DPP - Digital Product Passport
- Assets: bootloader/firmware images, device
- keys/PKI, update client/server, clinical data, wireless interfaces, debug ports, build pipeline.
- Adversaries: remote network attackers, proximity attackers (BLE/Wi-Fi), supply-chain/insider, physical with limited access.
- Representative threats (STRIDE): spoofed updates, key exfiltration, firmware tampering, rollback, DoS on therapy delivery, lateral movement via hospital networks.

VII. Acknowledgment

I would wish to express my heartfelt appreciation to all those who assisted me during the completion of this work. I appreciate my lecturers and instructors for their guidance, advice, and encouragement that allowed me to shape the

research and understand complex concepts in cybersecurity and medical devices.
I would also like to thank my friends and colleagues who shared their comments, shared resources, provided their time and feedback, and contributed to this work being more comprehensive and meaningful. My sincere appreciation to researchers whose work and resources I read, as they were the foundation of my learning and inspired my effort.
Lastly, I am grateful to all those who, in one way or another, shared their knowledge, assistance, or motivation, enabling me to finish this study successfully.

VIII. References

[1] A. Al-Khaldi and M. Rahrouh, "Cyber Risk and Threat Assessment Against the Security of Medical Devices and the Internet of Medical Things - A Theoretical Proposal," in 2024 Global Digital Health Knowledge Exchange & Empowerment Conference (gDigiHealth.KEE), Abu Dhabi, United Arab Emirates, 2024, pp. 1–5, doi: 10.1109/gDigiHealth.KEE62309.2024.10761780.

[2] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," IEEE Access, vol. 7, pp. 183339-183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[3] J. Doménech, S. Mhiri, M. Shuaib Siddiqui, and J. Pegueroles, "Preventive and Reactive Cybersecurity Techniques on IoT Devices in Healthcare Environments," in 2025 IEEE 11th International Conference on Network Softwarization (NetSoft), Budapest, Hungary, 2025, pp. 261-264, doi: 10.1109/NetSoft64993.2025.11080634.

[4] F. Stodt, P. Ruf, and C. Reich, "Blockchain-Enabled Digital Product Passports for Enhancing Security and Lifecycle Management in Healthcare Devices," in 2024 8th Cyber Security in Networking Conference (CSNet), Paris, France, 2024, pp. 44-51, doi: 10.1109/CSNet64211.2024.10851725.

[5] K. Taylor, A. Smith, A. Zimmel, K. Alcantara, and Y. Wang, "Medical Device Security Regulations and Assessment Case Studies," in 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), Denver, CO, USA, 2022, pp. 742-747, doi: 10.1109/MASS56207.2022.00116.

[6] M. Webster, "IoMT and Health Regulation," in Do No Harm: Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States. Wiley, 2021, pp. 73-84.

[7] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, "Attack Detection for Medical Cyber-Physical Systems-A Systematic Literature Review," IEEE Access, vol. 11, pp. 41796-41815, 2023, doi: 10.1109/ACCESS.2023.3270225.

[8] P. Udayakumar and R. Anandan, "Evaluation of Protocol-Centric IDS for the IoMT Leveraging ML Techniques," in 2024 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2024, pp. 546-551, doi: 10.1109/AIIoT61789.2024.10578945.

[9] T. Nusairat, M. M. Saudi, and A. B. Ahmad, "A Recent Assessment for the Ransomware Attacks Against the Internet of Medical Things (IoMT): A Review," in 2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE), Penang, Malaysia, 2023, pp. 238-242, doi: 10.1109/ICCSCE58721.2023.10237161.

[10] U. Jafar and H. A. Hussain, "Enhancing Cybersecurity in Healthcare Using Blockchain and IoMT-Integrated Framework for Mitigating Emerging Risks," in 2024 IEEE 7th International Symposium on Telecommunication Technologies (ISTT), Langkawi Island, Malaysia, 2024, pp. 144-149, doi: 10.1109/ISTT63363.2024.10750568.

[11] A. Bajpai, A. Maurya, and A. Yadav, "A Hybrid Approach for Enhancing Data Aggregation Security in the Internet of Medical Things," in 2023 14th International

Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10306533.

[12] J. Rajamäki, "Cybersecurity in Internet of Medical Things: Threats and Innovative AI-Driven Tools," in 2025 IEEE Medical Measurements & Applications (MeMeA), Chania, Greece, 2025, pp. 1-6, doi: 10.1109/MeMeA65319.2025.11068017.

[13] T. Revathi, K. Anbazhagan, and R. Kavitha, "Utilizing Deep Learning to Enhanced Security in the Internet of Medical Things via Intrusion Detection Systems," in 2024 International Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS), Bengaluru, India, 2024, pp. 1-6, doi: 10.1109/ICETCS61022.2024.10543626.

[14] U. Zukaib, X. Cui, C. Zheng, M. Hassan, and Z. Shen, "Meta-IDS: Meta-Learning-Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network," IEEE Internet of Things Journal, vol. 11, no. 13, pp. 23080-23095, Jul. 1, 2024, doi: 10.1109/JIOT.2024.3387294.

[15] D. Gautam, G. Thakur, M. S. Obaidat, K.-F. Hsiao, and P. Kumar, "Security Analysis and Improvement of Authenticated Key Agreement Protocol for Remote Patient Monitoring IoMT," in 2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), Beijing, China, 2024, pp. 1-8, doi: 10.1109/CCCI61916.2024.10736457.

[16] A. Akram, J. Akram, A. Alabdultif, A. Anaissi, and R. H. Jhaveri, "Secure and Interoperable IoMT-Based Smart Homes," *IEEE Consumer Electronics Magazine*, vol. 14, no. 4, pp. 100-105, Jul. 2025, doi: 10.1109/MCE.2025.3534442.

[17] S. Khan, M. Khan, M. A. Khan, M. A. Khan, L. Wang, and K. Wu, "A Blockchain-Enabled AI-Driven Secure Searchable Encryption Framework for Medical IoT Systems," *IEEE Journal of Biomedical and Health Informatics*, Early Access, 2025, doi: 10.1109/JBHI.2025.3538623.

IX. AUTHOR PROFILE

Umayangi Rajapaksha is an undergraduate student pursuing a B.Sc. (Hons.) in Information Technology specializing in Cyber Security at the Sri Lanka Institute of Information Technology (SLIIT). Her research interests include firmware integrity, penetration testing, machine learning-based intrusion detection systems, and vulnerability assessment. She is also active as a bug bounty hunter and has contributed to identifying security flaws in real-world applications.