Securing the Digital Lifeline: A Review of Firmware Integrity, Supply Chain Risks, and Penetration Testing in Next-Generation Medical Devices

A A I Nethmika
Faculty of Computing (Specializing in Cyber Security)
Sri Lanka Institute of Information Technology (SLIIT) Malabe, Sri Lanka

***Abstract*— Next generation medical devices increasingly operate within the Internet of Medical Things, improving care while expanding the attack surface. This review synthesizes research on three pillars that determine device resilience: firmware integrity, software supply-chain risk and penetration testing in clinical contexts. It summarizes evidence and techniques for trustworthy boot and authenticated software loading; analyzes update and maintenance practices for ling-lived devices, including risks inheriting from third party components; and distills lessons from foundational attack demonstrations on implantable and wearable systems that motivate safety aware testing. Cross cutting themes include the need for authenticated and traceable firmware updates; lifecycle transparency to accelerate vulnerability triage and adjunct protections such as external anomaly monitoring and secure auxiliary channels. The review concludes by outlining focused directions for future work; verifiable update pipelines for constrained platforms, lightweight attestation that preserves emergency access, automation of component transparency and vulnerability matching, hardening patterns for legacy deployments and standardized, bench-safe penetration testing methods that map directly to clinical impact.**

***Index Terms*— Medical device security, firmware integrity, software supply-chain risk, penetration testing, Internet of Medical Things, body are networks, radio frequency security, over-the-air firmware updates, anomaly detection, interoperability.**

I. INTRODUCTION

Next-generation medical devices increasingly operate within the Internet of Medical Things (IoMT), linking implantable and wearable systems with gateways and clinical backends. This connectivity improves monitoring, personalization and timeliness of care, but it also expands the attack surface and makes cybersecurity inseparable from patient safety [16][17]. Trustworthiness therefore shifts from a purely functional concern to a lifecycle problem that spans device software, communication paths and operational governance [7].

Foundational studies established that wireless (radio frequency) interfaces can be abused if not properly protected, demonstrating unauthorized telemetry access and command manipulation against implantable cardiac devices and insulin pumps under controlled conditions [8][9]. Systematizations and surveys since then have mapped common vectors across device communication stacks covering Body Area Networks (BANs) and Wireless Body Are networks (WBANs), pairing/ authentication and command integrity and emphasized that evaluation must be engineered to avoid clinical risk [6][10][11]. Together, these works motive safety aware penetration testing that is scoped, repeatable and tied to clinical impact.

The first pillar of resilience is **firmware integrity.** The literature converges in establishing trustworthy boot pathways, authenticated software loading and robust, signed over-the-air updates with formal methods proposed to expose defects early in development [1][4][14]. Analyses of safety critical failures in deployed devices further underlined why these controls matter: software and firmware faults recur in real world incident data and remediation in the field demands reliable processes and verification [3].

Ther second pillar is **software supply chain risk**. Networked device surveys and BAN/WBAN overviews highlight dependency exposure from third party code and communication modules as well as the maintenance challenges posed by long lived platforms [5]-[7]. Legacy software constraints can limit direct patching, increasing reliance on compensating controls and disciplined update planning [2]. Recent IoMT surveys argue for greater component level transparency and coordinated vulnerability triage across heterogeneous fleets [16][17].

The third pillar concerns **penetration testing in clinical contexts.** Beyond showing feasibility, research points to practical safeguards such as access control models tailored to implantables, external anomaly monitors that can observe and bock malicious traffic without altering device firmware and auxiliary physical channels to authenticate sensitive operations that both inform testing and reduce residual risk in operation [11]-[13]. Because IoMT systems span device-to-gateway-to-

cloud paths, assurance must be end-to-end and repeatable at scale [16][17].

The review synthesizes these three pillars to clarify techniques for assuring **firmware integrity,** approaching for managing **supply-chain risk** in long lived connected devices and methods for conducting **penetration testing** that protect safety. The goal is to organize what is known, identify gaps and outline focused directions that advance secure design, maintenance and evaluation of modern medical devices [1]-[17]

II. RESEARCH STATEMENT/ OBJECTIVES

This paper reviews the literature on cybersecurity in next generation medical devices, with particular emphasis on firmware integrity, software supply chain risk and penetration testing in clinical contexts. While advances in connectivity and embedded intelligence have enabled safer, more personalized and more efficient healthcare, they have also expanded the attack surface and increased the complexity of securing medical technologies. Addressing these challenges requires a comprehensive understanding of device firmware assurance, transparent software supply chains and security testing practices that do not compromise the safety of the users (including patients).

The primary objective of this review is to synthesize current research and standards to clarify how these three domains collectively influence the resilience of medical devices. The review also seeks to identify existing gaps in literature and provide insights for manufacturers, regulators, healthcare providers and research on how to improve device trustworthiness in an increasingly connected healthcare environment.

To guide this review, the following research questions are addressed:

- What techniques best ensure firmware integrity and authenticity across the medical device lifecycle?
- Which framework and standards most effectively reduce software supply chain risk in connected healthcare systems?
- How should penetration testing be scoped and executed to protect-safety critical functions while meeting regulatory expectations?

III. REVIEW OF THE LITEREATURE

A. Firmware Integrity

1) Why Firmware Integrity Matters in Next Generation Devices

Safety critical devices recall, and adverse event reports show that unsafe or tampered firmware can directly endanger patients' safety. Alemzadeh et al. analyzed failure data and found recurring firmware and software faults in critical devices highlighting the importance of lifecycle assurance [3]. Industry experience has also demonstrated large scale remote update campaigns, reinforcing the need for reliable firmware update mechanism and verification processes [14].

2) Secure/Measured Boots and Roots of Trust

In next generation IoMT platforms, integrity begins at boot. Altawy and Youssef frame the tradeoff between strong cryptographic enforcement and clinical availability, emphasizing that secure boot must coexist with emergency override mechanisms [4]. Surveys of IoMT systems also stress that trusted execution and authenticated boot are foundational for preventing persistent malware and maintaining patient safety [16][17].

3) Code Signing, OTA Updates and Rollback Protection

Modern devices must support secure over-the-air (OTA) updates. Hudson and Clark note that interoperability initiatives and standards such as IEEE P2621 are beginning to define secure update expectations, including trust anchors, identity management and rollback prevention [14]. IoMT surveys similarly highlight the importance of authenticated update distribution and coordinated key management [16].

4) Formal Methods and Software Assurance

Li et al. demonstrate how model checking and theorem proving can uncover latent defects in device software, proposing formal verification to complement conventional testing for critical control logic [1]. Such approaches could make future firmware pipelines more trustworthy before deployment.

5) Legacy Software and Long-Lived Devices

Legacy software in ling lived devices remains one of the hardest problems. Tervoot et al. Categorize mitigation strategies such as cryptographic tunneling and compensating network controls, offering practical solutions for devices that cannot be patched in the field [2].

6) Runtime Anomaly Detection and External Monitors

When strong integrity cannot be guaranteed, runtime monitoring offers a compensating safeguard. Zhang et al. proposed MedMon, a wireless anomaly detector that passively monitors device traffic and blocks malicious commands, enabling protection without modifying deployed firmware [13].

7) Synthesis and Implications

Across classic and recent work, the literature converges on four pillars for firmware integrity. Secure/ measured boots with hardware roots of trust, signed and authenticated OTA updates with rollback protection, formal verification and rigorous testing of control logic and compensating measures for legacy devices such as runtime monitoring and protocol wrappers. While promising solutions exist, more research is needed too:

- Verify update pipelines with formal methods [1][4].
- Design lightweight attestation protocols that balance availability with cryptographic assurance [4][16].
- Develop standardized hardening patterns for legacy software [2]
- Certify runtime monitoring systems like MedMon so they can be safely deployed in clinical environments [13].

B. Supply Chain Risk and Software Bill of Materials

1) The Expanding Attack Surface

Modern medical devices are increasingly assembled from a mix of proprietary firmware, third party drivers, open-source software components, and wireless modules. This complexity introduces multiple potential entry points for attackers. Yaqoob et al [5] surveyed vulnerabilities in networked medical devices and concluded that third party dependencies are a primary source of software flaws. Similarly, Movassanghi et al. [6] highlighted security gaps in Wireless Body Area network protocols, which are often embedded in commercial off the shelf modules.

2) Key Supply Chain Risks

Risk Category	Description	Impact on Medical Devices
Vulnerable third-party Libraries	Outdated or unmaintained libraries may contain known CVEs	Allows privilege escalation or remote code execution
Counterfeit/Cloned hardware	Tampered components in the hardware supply chain	Loss of integrity, possible backdoors
Lack of SBOM Transparency	No inventory of components or versions used	It is difficult to patch quickly when vulnerabilities are disclosed
Dependency on Legacy OS	Old operating systems remain unpatched	Expands attack surface and compliance risk

3) SBOM as a Transparency mechanism

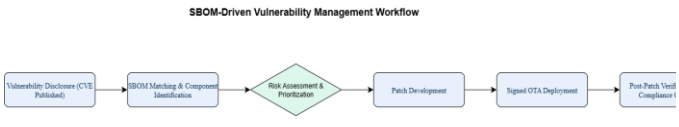
The concept of Software Bill Materials (SBOM) has emerged as solution to improve supply chain visibility. Ghubaish et al [16] and Sun et al [17] both argue that component level transparency is essential for vulnerability management. Especially in IoMT environments where devices remain in service for main years.

An SBOM enable:

- Rapid identification of affected devices when a vulnerability is published.
- Prioritization of patch deployment.
- Better coordination between manufactures, hospitals and regulators.

4) Flow of Vulnerability Management

Figure 1



SBOM-driven workflow:

Figure 1 shows how Software Bill of Materials (SBOM) data operationalizes vulnerability management in next generation of devices. When a vulnerability is disclosed (CVE), the SBOM enables rapid impact analysis to locate affected components and devices. This directly addresses third party and module dependencies highlighted in medical/IoMT surveys [5][6][16][17] and supports broader device trustworthiness goals [7]. The workflow also reflects emerging expectations for authenticated traceable updates in connected health systems (e.g. signed OTA and post deployment auditability) [14].

Starting **with Vulnerability Disclosure (CVE Published)** the operator performs **SBOM Matching & Component Identification** to determine exposure. **A Risk Assessment & Prioritization** follows weighing severity, exploitability and patient safety impact to triage fixes. Engineering then executes **Patch Development**, followed by **signed OTA Deployment** to ensure integrity and prevent tampering in transit. Finally, **Post-Patch Verification & Compliance Check** confirms successful remediation and record audit logs to support regulatory and clinical assurance [5][7][14][16][17].

This workflow clarifies where automation is most needed (continuous SBOM generation, real time CVE matching and risk scoring) and where governance is critical (cryptographic update pipelines and auditable verification) [2][7][14][16][17].

5) Standards and Regulatory Drivers

Standards such as IEE P2621 [14] and regulatory frameworks like the FDA's premarket cybersecurity guidance now expect manufacturers to document and maintain SMOMs throughout the lifecycle. Zhang et al. [7] point out that trustworthiness in medical devices is not just a matter of secure design but also of ongoing maintenance which SBOM enables.

6) Implication for Research

Despite growing interest, many challenges remain:

- **Automation:** Research is needed to automate SBOM generation for embedded devices without adding excessive overhead [5][16][17].
- **Real Time Risk Scoring:** Tools should be developed to cross check SBOMs with vulnerability databases in near real time [7][16][17].
- **Supply Chain Attestation:** Lightweight methods for verifying the authenticity of hardware and firmware components during manufacturing could further reduce risks [2][7][14].

C. Penetration Testing in Clinical Contexts

1) Why penetration testing Is different for medical devices.

Penetration testing in safety critical devices must balance rigorous security evaluation with patient safety and clinical availability. Early, influential demonstrations showed that wireless interfaces and telemetry channels can be abused to alter therapy or exfiltrate data, establishing both the feasibility of attack and the need for safety aware test practices [8][9]. Systemization and survey work since then has mapped common vectors (telemetry, RF/BAN protocols, evoke pairing/auth) and

framed penetration testing within boarder device trustworthiness requirements [7][10].

2) Classic demonstration (foundation evidence)

- **Pacemakers/ICDs:** Halperin et al. used software radio to analyze and manipulate device telemetry and proposed zero power defenses work that became a touchstone for safety aware evaluation [8].
- **Insulin pumps:** Li et al demonstrated active and passive RF attacks and discussed countermeasures highlighting the need for scoped and controlled penetration setups [9]
- **Synthesis:** These studies remain the canonical rationale for formalizing medical penetration testing: attack feasibility is real, but testing can be engineered to avoid patient harm and unintended clinical disruption [8][9][10].

3) What to test: interfaces, controls and mitigations

Surveys on implementable devices and WBANs (Wireless Body Area Networks) identify recurring weaknesses in device access control, pairing and telemetry confidentiality/integrity [6][10][11]. In parallel, "trustworthiness" perspectives emphasize that penetration testing should be paired with runtime safeguards and update integrity so that findings translate into durable risk reduction [7]. Research prototypes illustrate two safety aware directions:

- **Out of band / physical side channels:** SecureVibe established an auxiliary vibration channel to authenticate interactions, reducing reliance on vulnerable RF alone [12].
- **External anomaly monitors:** MedMon passively observes wireless traffic to detect/jap anomalous commands, enabling protective oversight without modifying deployed firmware [13].

4) How to test safely: environments and scope

Systematization work recommends **controlled testbeds, emulated/bench setups or device twins** to avoid patient risk during penetration testing. Tests should focus on well scoped objectives (e.g. authentication bypass, command integrity, replay) and be traceable to clinical impact [10]. IoMT surveys reinforce the need to examine **end to end** connectivity and to verify that fixes (e.g. signed updates, access control changes) hold under realistic operating conditions [16][17]. Interoperability guidance further signals that authenticated, auditable updates paths are now part of the evaluation baseline [14].

5) A current topic: penetration testing for IoMT-scale connectivity.

Recent IoMT reviews describe a landscape where large fleets of connected devices and heterogenous BAN/WLAN/wan links expand the attack surface and increase the need for repeatable, safety-aware penetration testing that considers gateways and cloud interfaces. Not just implants / wearables in isolation [16][17]. In this context, research activity concentrates on,

i. Surveying/ penetration test – oriented analyses of access control models for implants [11].
ii. BAN protocol exposure and mitigations [6]
iii. Designs for auxiliary or external safeguards that enable safe experimentation and post deployment protection [12][13].

6) What the literature agrees on (synthesis)

Across classic demonstration and recent surveys four themes recur:

i. Feasibility of remote misuse through telemetry/ BAN channels [8][9][10]
ii. The centrality of access control and authenticated commands in implants and wearables [11]
iii. Value of safety aware penetration testing setups (benchtop, emulation, monitored RF spaces) to avoid clinical risk [10].
iv. Pairing penetration testing with runtime/adjacent mitigation (external monitors, auxiliary channels) and with trusted update mechanisms to ensure findings translate into lasting protections [7][12][13][14][16][17].

7) Implication for research

- **Safe penetration testing frameworks:** Define repeatable, bench grade penetration testing procedures and metrics tied to clinical impact (e.g. command integrity, therapy perturbation thresholds) in line with survey guidance on IMD/ BAN risk and IoMT contexts [6][10][16][17]
- **Adjunct protections:** mature external monitors and auxiliary channels (e.g. MedMon – style physical side channel anomaly detection) into deployable safeguards that both enable safe testing and reduce field risk [12][13].
- **From findings to fixes:** Integrate penetration testing outputs with trustworthy update and verification paths, aligning remediation with authenticated and auditable deployments highlighted in interoperability guidance and trustworthiness analyses [7][14].

IV. FUTURE RESEARCH

1) Provable update pipelines for safety critical firmware

Develop formally specified and verified state machines for code signing, rollback prevention and key rotation on constrained IMD/ wearable MCUs, extending early formal methods work into end-to-end OTA workflows [14][16].

2) Lightweight attestation with clinical overrides

Design remote attestation and measured/ secure boot schemes that preserve emergency access and availability requirements unique to medical devices, building in IMD security trade off analyses and IoMT survey guidance [4][16][17]

3) Automated SBOM for embedded stacks and real time scoring

Create tools that continuously generate SBOMs from embedded. RTOS builds and maps them to vulnerability feeds (CVE/NVD) for real time triage in healthcare fleets [5][16][17]. Integrate outputs with device trustworthiness process [7].

4) Hardening patterns for legacy devices and ling service lives

Systematize compensating controls - cryptographic tunneling/ wrappers, network segmentation and runtime monitor for fielded devices that cannot be fully patched, with lifecycle evidence of risk reduction [2][3][13]

5) Safety aware penetration testing frameworks and benchmarks.

Define repeatable penetration testing procedures, bench/emulation testbeds and metrics tied to clinical impact (e.g. command integrity and therapy perturbation thresholds), grounded in canonical attack demonstrations and systematizations of IMD/BAN risks [6][8][9][10][11][16][17].

6) Adjunct protections: external monitors and auxiliary channels

Advance detection response coverage via certified external anomaly monitors and physical side channels. Quantify efficacy, false positive ceilings and integration pathways for clinical deployment [12][13].

7) Fleet scale governance for secure OTA and interoperability.

Study operational controls for authenticated, auditable updates and post deployment verification across diverse wearables/implants and hubs, aligning with interoperability expectations in connected care [14][16][17].

These directions align with **firmware integrity, supply chain risk and safe penetration testing** and target gaps repeatedly surfaced in the literature [1]-[17].

V. CONCLUSION

Next generation medical devices increasingly operate as part of the Internet of Medical Things (IoMT) linking implantable and wearable sensors with hospital systems and cloud services. This connectivity improves care but widens the attack surface, making cybersecurity inseparable from patient safety [16][17]. The literature reviewed in this paper shows that effective protection hinges on three pillars which are firmware integrity, software supply chain risk management and carefully scoped penetration testing.

On firmware integrity, studies coverage on establishing trustworthy boot pathways, authenticating software loads and deploying signed over the air updates; complementary assurance methods (e.g. formal verification) help surface defects before deployment, while failure analyses underscore why these control matter in practice [1][3][4][14]. Supply chain risk appears in two forms. Those are vulnerabilities inherited through third party components and protocols and long lifetimes of deployed systems that complicate patching. Surveys of networked medical devices and wireless/Body Area Networks (WBAN/BAN) emphasize dependency exposure and lifecycle constraints that must be addressed with transparency and maintainability in mind [5][6][7]. The attack demonstrations on pacemakers/ICDs and insulin pumps provide foundational evidence that radio frequency (RF) channels can be misused, motivating penetration testing that is rigorous yet clinically safe.; systematizations, access control surveys and defense prototypes (e.g. external anomaly monitors and auxiliary physical channels) outline practical ways to evaluate and harden devices without endangering patients [8]-[13].

Taking together, the field points toward several actionable priorities. First make update and rollback logic as robust as the cryptography that protects it and verify that logic early [1][14]. Second, improve supply chain visibility and maintenance planning for ling lived devices. Especially where legacy software cannot be fully replaced [2][5][6][7]. Third, embedded penetration testing within controlled benches, emulations and monitored environments and pair findings with mitigations that persist after testing stronger access control authenticated commands and runtime oversight [10]-[13]. Finally, because IoMT systems span device to gateway to cloud paths, assurance must be ended to end and repeatable at fleet scale [16][17].

In short, the literature makes clear that securing modern medical devices is not a single mechanism but a coordinated practice across design, updates, supply chain and evaluation. Advancing trustworthy firmware, reducing inherited risk and institutionalizing safety, evidence driven penetration testing will be central to protecting patients and sustaining clinical confidence in increasingly connected care.

ACKNOWLEDGEMENT

I thank my course lecturer, Mr. Kanishka Yapa, and lab instructors for guidance and feedback during this review. I also appreciate the support of the university library and IT staff for enabling remote access to IEEE Xplore and related database. Part of the drafting and editing process were assisted by an AI language model (ChatGPT). All the selection of sources, analysis and final decisions are author's own. Figures were created by the author using draw.io and Canva. No external funding was received, and the author declares no competing interests.

REFERENCES

[1] C. Li, A. Raghunathan and N. K. Jha, "Improving the Trustworthiness of Medical Device Software with Formal Verification Methods," in IEEE Embedded Systems Letters, vol. 5, no. 3, pp. 50-53, Sept. 2013, doi: 10.1109/LES.2013.2276434.

[2] T. Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. Olabarriaga and H. Marquering, "Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review," in IEEE Access, vol. 8, pp. 84352-84361, 2020, doi: 10.1109/ACCESS.2020.2984376.

[3] H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk and J. Raman, "Analysis of Safety-Critical Computer Failures in Medical Devices," in IEEE Security & Privacy, vol. 11, no. 4, pp. 14-26, July-Aug. 2013, doi: 10.1109/MSP.2013.49.

[4] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," in IEEE Access, vol. 4, pp. 959-979, 2016, doi: 10.1109/ACCESS.2016.2521727.

[5] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3723-3768, Fourthquarter 2019, doi: 10.1109/COMST.2019.2914094.

[6] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith and A. Jamalipour, "Wireless Body Area Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1658-1686, Third Quarter 2014, doi: 10.1109/SURV.2013.121313.00064.

[7] M. Zhang, A. Raghunathan and N. K. Jha, "Trustworthiness of Medical Devices and Body Area Networks," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1174-1188, Aug. 2014, doi: 10.1109/JPROC.2014.2322103.

[8] D. Halperin et al., "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 2008, pp. 129-142, doi: 10.1109/SP.2008.31.

[9] Chunxiao Li, A. Raghunathan and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO, USA, 2011, pp. 150-156, doi: 10.1109/HEALTH.2011.6026732

[10] M. Rushanan, A. D. Rubin, D. F. Kune and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 524-539, doi: 10.1109/SP.2014.40.

[11] L. Wu, X. Du, M. Guizani and A. Mohamed, "Access Control Schemes for Implantable Medical Devices: A Survey," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1272-1283, Oct. 2017, doi: 10.1109/JIOT.2017.2708042.

[12] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha and A. Raghunathan, "Vibration-based secure side channel for medical devices," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2015, pp. 1-6, doi: 10.1145/2744769.2744928.

[13] M. Zhang, A. Raghunathan and N. K. Jha, "MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection," in IEEE Transactions on Biomedical Circuits and Systems, vol. 7, no. 6, pp. 871-881, Dec. 2013, doi: 10.1109/TBCAS.2013.2245664.

[14] F. Hudson and C. Clark, "Wearables and Medical Interoperability: The Evolving Frontier," in Computer, vol. 51, no. 9, pp. 86-90, September 2018, doi: 10.1109/MC.2018.3620987.

[15] G. Suciu, M. Anwar, A. Ganaside and A. Scheianu, "IoT time critical applications for environmental early warning," 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Romania, 2017, pp. 1-4, doi: 10.1109/ECAI.2017.8166451.

[16] Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," in IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8707-8718, 1 June1, 2021, doi: 10.1109/JIOT.2020.3045653.

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

AUTHOR PROFILE

Aluthwala Acharige Isindu Nethmika is an undergraduate in Information Technology specializing in Cyber Security at the Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka. Research interests include medical device security; firmware integrity and software assurance, software supply-chain risk and transparency (Software Bill of Materials, SBOM) and safety focused penetration testing for connected and implantable systems (IoT/IoMT)