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

Pasan Thedasara Jayarathna, Sri Lanka Institute of Information Technology (SLIIT)

Abstract: The Internet of Medical Things (IoMT) integrates smart technologies into devices for tracking a patient’s condition progressively and improving clinical outcomes, thus transforming modern healthcare. Despite its benefits, IoMT devices face serious cybersecurity challenges for maintaining the integrity of firmware, mitigating supply chain hardware and software vulnerabilities, and executing reliable penetration testing. This article focuses on the peer IoMT device cybersecurity challenges of forgery countermeasures and abusive changes attack firmware validation and explores recent efforts to protect advanced medical devices by penetrating test the IoMT devices. It also analyses blockchain based frameworks on augmenting the transparency and responsibility relating to healthcare supply chain. As well, the absence of the penetration testing methodology on the Internet of Medical Things (IoMT) is discussed to demonstrate the presence and fixing of the critical vulnerabilities of the healthcare critical system. The findings highlight the need for IoMT devices' active countermeasures in the healthcare’s critical environment and the need for a flexible cybersecurity approach for patient, healthcare personnel, and the medical systems safety.

Index Terms - Firmware for the Internet of Medical Things (IoMT), Blockchain technology, Cybersecurity measures, Medical Devices, Risk Mitigation strategies, Healthcare Supply Chain management, Smart Contracts.

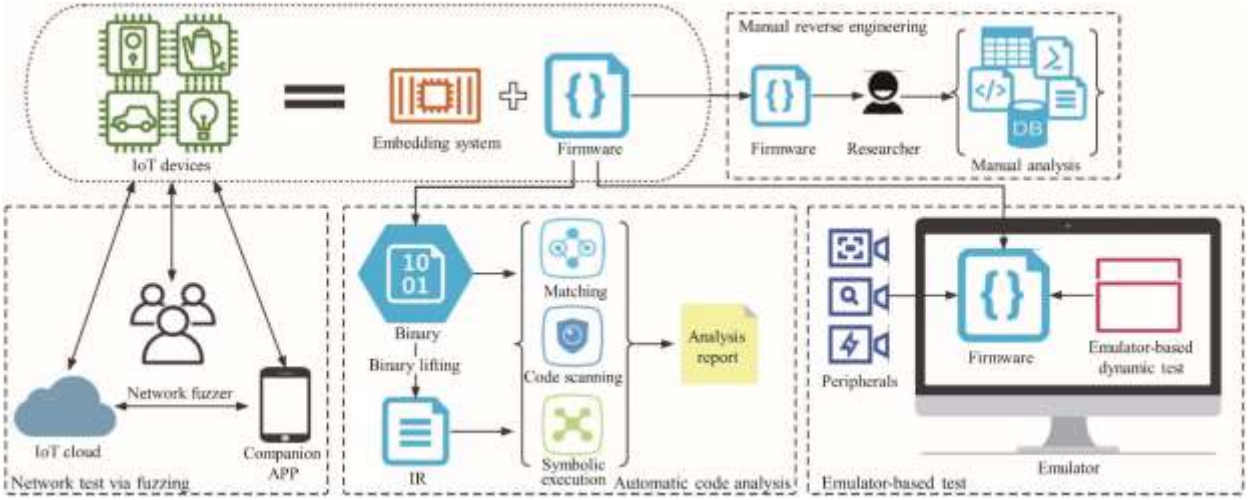
1. Introduction:

The swift digital advancement in the healthcare industry has resulted in the extensive implementation of the Internet of Medical Things (IoMT), which currently serves a vital function in healthcare service delivery. Ongoing patient surveillance, prompt diagnosis, and robotic procedures have improved clinical results. The increasing interconnectedness is expanding the attack surface, hence presenting significant cybersecurity vulnerabilities that jeopardize patient safety and the healthcare system.

Among the critical threats is the breach of firmware integrity which allows adversaries to exploit unmonitored updates to introduce malicious code or change the functioning of devices. The medical supply chain also poses vulnerabilities to the device’s integrity due to counterfeit parts, unmonitored software updates, and poor oversight of vendors. Furthermore, while healthcare IoT is an underdeveloped domain, its fundamental IT security measure of penetration testing lacks tailored security evaluation frameworks that prioritise patient safety.

This research offers a comprehensive examination of current frameworks that tackle these issues,

concentrating on (1) Firmware Integrity, (2) Supply Chain Risks, and (3) Penetration Testing.
By analyzing collaborative research, identifying gaps, and clarifying ongoing difficulties, researchers want to develop a comprehensive strategy to enhance the security and resilience of future medical devices.



2. Research Objectives:

1. Analyze the primary challenges and countermeasures related to maintaining firmware integrity in medical devices, emphasizing secure boot, authenticated updates, and runtime protection techniques.
2. Analyze security vulnerabilities in the medical device supply chain, focusing on the infiltration of counterfeit components, malicious software updates, and insufficient vendor management practices.
3. Evaluate the potential of blockchain technology to improve supply chain security, increase transparency, and provide reliable data traceability within healthcare systems.
4. Assess and compare contemporary penetration testing methodologies designed for healthcare IoT devices, focusing on their significance, limitations, and effectiveness in detecting vulnerabilities while safeguarding patient safety.
5. Identify significant research deficiencies and highlight potential pathways to bolster the robustness of medical IoT systems, including recommendations for interdisciplinary collaboration among researchers, regulators, and healthcare practitioners.

3. Literature Review

3.1 Firmware Integrity

As illegal code execution can severely disrupt essential functions, firmware security emerges as a critical aspect of medical device protection. As referenced in works by Bertino and Feng, the enforcement of cryptographic firmware, secure trust anchors, hardware lifecycles, and runtime surveillance work optimally when concatenated in a layered approach, bending the device towards layered defensive architecture [1][5].

Through a secure boot, the execution of illegal code can be mitigated when the firmware is cryptographically signed. Sun and Feng have highlighted in their works the vulnerabilities involving the injection of unsigned firmware code through the Internet of Medical Things, and how the infantile security policies aid the injection of unsigned code through proprietary protocols. Feng shows the need for lightweight validation and secured verification methods, such as elliptic-curve signatures, in their works for constrained IoT and Medical devices [1][2].

The IEEE Heterogeneous Integration Roadmap sketches the Integrative Circuits and IoT Devices with the Trusted Platform Modules, the Physically Unclonable Functions, and split manufacturing as hardware rooted trust and undermines firmware, reverse engineering, and hardware Trojans [3]. These frameworks increase the security of remote attestation and secure key storage, greatly amplifying trust and assurance when compared to only software measures. These methods limited to software only, as argued by Sun et al. are insufficient in adversarial healthcare contexts [1].

Embedded security measures enhance the security posture of devices when combined with lifecycle-oriented frameworks.

The Building Code for Medical Device Software Security (BCMDSS) prescribes signed updates, enhanced key storage, whitelisting, and tamper-evident logging for the entire device lifecycle [4]. Rushanan et al. noted the lack of or poor authentication mechanisms in Implantable Medical Devices (IMDs) and Body Area Networks (BANs) have predisposed them to eavesdropping and denial-of-service attacks which highlights the need for update standardisation [5].

Detection mechanisms also accompany such technologies to identify attacks at the firmware level. Feng et al. described such techniques as fuzzing, symbolic execution, and binary lifting as identifying update handler and bootloader vulnerabilities. Moreover, some detection methods monitor for volatile system calls, power, or traffic and classify them as manipulative efforts [2]. However, these approaches face limitations due to scale, high false positive rates, and adaptability to low resource implants.

To conclude, maintaining firmware integrity requires an uncompromised security architecture involving cryptographic signing, trust anchors in hardware, lifecycle-driven processes, and advanced detection mechanisms. There exist critical gaps in lightweight attestation for ultra-constrained devices, reproducible validation techniques, and the creation of cross-border safety frameworks which are essential to protect the firmware of next-generation medical devices that function as digital lifelines in today's healthcare.

3.2 Supply Chain Risks

The scope of potential vulnerabilities within healthcare supply chains has expanded with the globalisation of medical device and pharmaceutical production. The increase of IoMT device applications poses further risks and threats to patient safety, the integrity of medical devices, and healthcare operations. The primary threats include the presence of counterfeit parts, lax controls on software updates, insufficient controls on vendors, and lax regulation. The attributes of transparency, immutability, and decentralized trust position blockchain technology as a widely advocated potential solution.

A. Fraudulent Components

The healthcare industry has dangerously slackened the controls it imposes on supply chains. Goswami et al. documented a rise in counterfeit medical devices, especially during the COVID-19 pandemic when PPE and diagnostic kit fraud peaked. This form of fraud poses the risk of devices malfunctioning and, in more extreme cases, causing direct harm to patients. To protect and mitigate healthcare fraud, the FDA, WHO, and other regulatory bodies have promoted greater supply chain controls and enhanced traceability.

B. Malevolent Updates and Vulnerabilities

The execution of detrimental updates, whether unintentionally applied or intentionally designed, constitutes a significant problem. Malefactors may exploit inadequate oversight of updates to introduce detrimental patches that alter equipment, leading to its disablement or failure.

Updating processes for pacemakers and insulin pumps have no regulatory oversight and are considered potential security gaps in medical devices. Such cases emphasise the need for reliable and auditable updating mechanisms.

C. Blockchain for Risk Mitigation

Blockchain technology can securely and redundantly record and authenticate transactions in supply chains, ensuring information integrity while preserving secrecy. It has been utilized in pharmaceutical and vaccine supply chains to improve traceability, auditability, and fraud prevention. Blockchain has also been beneficial in clinical trials for the transparent exchange of tamper-proof data among many stakeholders. Unlike central systems, blockchain reduces the risk of single-point failures due to the distributed nature of the system, and in this case, critical patient data not being stored on-chain.

D. Management of Vendor Risk

Vulnerabilities stemming from vendors continue to pose a considerable risk, particularly because of the reliance on foreign vendors with subpar standards of quality and regulation. Several companies do not have dedicated vendor risk management systems. Blockchain can provide immutable audit trails and assure the inclusion of only verified vendors to the supply chain, thus solving these issues of unregulated vendor risk management, providing vendor risk management systems.

E. Regulatory and Compliance Deficiencies

Cyclically connected medical devices often remain unregulated due to a lack of adequate primary rules.

Current IoMT ecosystems are said to be inadequately protected from abuse of surveillance technologies by existing IoMT policies. The provisions in HIPAA and GDPR concerning auditing and data sharing are supported by blockchain technology. However, blockchain's widespread adoption would need to be accompanied by holistic, uniform policies spanning across the entire ecosystem.

F. IEEE Standards for Blockchain in Healthcare

To address the deployment challenges and provide the best-use practices of blockchain in healthcare, the IEEE P2418.6™ and IEEE P2418.1™ have been set by IEEE Standards Association (IEEE-SA). These standards define borderless and secure adoption of blockchain in healthcare systems by addressing core requirements and technologies like privacy, security, and flexibility.

The healthcare supply chain faces complex and fluid threats like the infiltration of counterfeit goods, unverified updates, and lack of regulatory oversight. Blockchain technology can mitigate these vulnerabilities by providing transparency, immutability, and vendor verification. However, blockchain technology needs to be more scalable, incorporate AI for predictive oversight, and have universally cohesive policies.

Future Directions

More work needs to be done in the field of healthcare to enhance blockchain technology's scalability, interoperability, and secure healthcare transactions by making vendor audit and data provenance more stringent.

To manage supply chain risk and protect healthcare systems from the ever-evolving cyber risks, ongoing collaboration among industry partners, regulators, and patients, as well as the application of open industry standards like blockchain, will be essential.

Additionally, future studies should analyse the potential of AI and machine learning in forecasting system weaknesses and in the autonomous identification of deviations in blockchain-based systems. AI's capability to strengthen blockchain technology's application in real-time supply chain oversight can help in the timely detection of discrepancies, ranging from counterfeit items to insidious software updates. Further, determining the potential of incorporating blockchain technology with the next generation of encryption methods will be of utmost importance to guarantee the confidentiality and integrity of shared data in decentralised healthcare systems. Collaborative initiatives aimed at establishing uniformity in the application of blockchain in healthcare are equally imperative to enable its universal acceptance and to sophisticate its alignment with the contemporary healthcare systems.

3.3 Penetration Testing

A proactive strategy for the cybersecurity of modern medical equipment and healthcare systems entails penetration testing (pentesting), which identifies and mitigates security flaws prior to their use. The swift integration of intelligent healthcare technology, including virtual surgical systems, telemedicine, patient monitoring systems, and wearable medical devices, has markedly heightened the risk of cyberattacks. Pentesting enables researchers and practitioners to review actual cyber-attack simulations, thereby evaluating system resilience and proactively identifying vulnerabilities [14].

Remote surgery IoT medical devices, wearables, and telemedicine are vulnerable to numerous dangers, including data corruption, device hijacking, and malware infiltration via mobile applications. These dangers present significant concerns, including the illicit modification of surgical instruments and the unauthorized manipulation of essential patient records [14], [15]. A customized framework for IoT healthcare ecosystems is essential to mitigate these hazards [14].

Such frameworks will typically have modules for device-level testing, network resilience evaluation, and data validation, to constitute the architectural architecture. Unlike general security tests, healthcare penetration testing must include the unique privacy, patient safety, system availability, and patient safety benchmarks. Furthermore, penetration testing helps to comply with regulations such as HIPAA and GDPR, which are designed to evaluate confidentiality breaches and security assessments without compromising safeguarding [15]– [17].

A. Framework Design

A healthcare IoT modular platform is based on a healthcare stratified architecture with layered security which is unique to the domain.

It includes SAST, DAST, and vulnerability scanning for devices and firmware along with communications protocol assessment. [14, 18] More recent proposals advocate for automated testing tool implementation within the frameworks for sustained oversight and real-time anomaly identification, which is crucial in sensitive healthcare environments [13].

B. Performance Evaluation Metrics

- The efficacy of penetration testing is evaluated via quantitative criteria such as:
- Penetration Success Rate (PSR): quantifies the probability of successful hack.
- Path Coverage (PC): measures the extent to which the framework tests for attack vectors.
- System Disruption Rate (SDR): assesses the potential service stoppage due to attack simulations.
- Lower values of both PSR and SDR indicate better defence, but higher values indicate the need for greater security attention.

C. Automated Penetration Testing

The scale and complexity of current healthcare IoT ecosystems necessitate automation. Automated penetration testing ensures perpetual, consistent, and cost-effective security assessments, reduces the chances of human error, and accelerates the process of vulnerability identification. Automated systems are also able to quickly assess new patches and respond to emerging threats, thereby reducing the potential exposure time. [14, 18]

D. AI Integrated Penetration Testing

AI is being integrated into penetration testing focused on healthcare, with an increasing trend. Approaches such as Learning Vector Quantisation (LVQ) and Probabilistic Neural Networks (PNN) allow penetration testing systems to adapt to new vulnerabilities as they emerge. As an example, PNNs can monitor logs and device interactions in real-time to detect possible violations that suggest the presence of cyberattacks.

Advanced AI techniques can automate penetration testing by implementing sophisticated techniques and strategies used by adversaries, such as data poisoning, evasion attacks, and insider threats. Such systems not only find vulnerabilities, but they also provide recommendations to address these vulnerabilities, thus reducing the need for human input and increasing scalability. AI-enabled penetration testing adjusts automatically to the changing threats, thus strengthening the security posture of healthcare IoT systems [19].

4. Future Research

While next-generation medical devices have improved security features, other forms of security, such as penetration testing techniques, scalability of blockchain, and the implementation of AI-based IoT security devices still have gaps. Addressing these gaps and inadequacies requires synchronized legislative and technological research on healthcare cybersecurity.

I. AI Integrated Cybersecurity Solutions for Threat Detection and Management

AI and machine learning have demonstrated immense capabilities in vulnerability detection, but the poorly optimised models still require improvement for executing in real-time systems. Lightweight, adaptive, real-time AI systems that detect and respond to emerging risks in a dynamic fashion would require fewer computing resources and real-time systems.

II. Healthcare Supply Chain Management and Blockchain Technology

Blockchain has emerged as a viable instrument for assuring traceability and transparency in the healthcare supply chains; however, scalability of the technology remains a challenge. Existing blockchain systems have limited capacity to handle large datasets and transaction volumes of medical supply chains. Future research should focus on the development of blockchain interoperability and scalability in other systems for real-time secure tracking of devices and consistent data across the healthcare systems.

III. Absence of Global Application of AI Penetration Testing Framework

The global deployment of AI penetration testing frameworks and their implementation in blockchain technology is hindered by the absence of regulatory guidelines. Concerns with IoMT device security, including adherence to HIPAA, GDPR, and other pertinent regulations, must emphasize lifecycle management and backward compatibility with outdated devices. This would enhance confidence among healthcare providers and regulators while advancing interoperability.

IV. Integration of Real-Time AI and Blockchain

The utilization of AI for anomaly detection and blockchain for the immutable storing of data in the continuous monitoring of medical devices presents a robust solution. Future research should concentrate on creating systems that integrate diverse technologies to facilitate real-time autonomous danger assessment and mitigation in dynamic healthcare settings.

V. Security for Devices with Limited Resources

Medical wearable and implantable sensors are often memory, processing, and energy constrained. These devices are often targeted with conventional security approaches. Research into lightweight cryptographic systems, anomaly detection, and attestation protocols for ultra-constrained environments must be prioritised.

VI. Security and Awareness from the End User Perspective

Behavior and technology both shape cybersecurity in healthcare. User negligence and unawareness of risks is the root of numerous security breaches. Enhanced ease of use along with clear step-by-step training guides for doctors, patients, and other relevant parties, must be implemented and supported for safe handling of medical IoT devices. Such training should be an integral part of the management procedures IoT devices in the medical field.

VII. Automated Threat Response Mechanisms

The next generation of medical IoT devices must incorporate an automated threat detection and response system that can instantly contain and mitigate threats in real time. Future research should focus on the design of AI self-healing systems that can respond to new patients' risks and adapt to the newly discovered threats while maintaining patient safety and minimising medical service interruptions.

VIII. Interdisciplinary Collaboration and Regulatory Frameworks

To comprehensively secure healthcare IoTs, there is a research gap that needs to be filled with strategies that address the issues of collaboration between healthcare professionals, IoT device developers, cybersecurity professionals, and governmental regulatory bodies. Given the concepts of patient safety and data privacy, future research should focus on finding ways to reconcile the global fragmented approach with adaptable and comprehensive legislation.

5. Conclusion

This investigation has examined the daunting cybersecurity challenges of next-generation medical devices alongside issues of firmware security, supply chain risks, and the application of penetration testing methodologies. The study pointed out that firmware security is the most critical aspect of device security and must be protected with strong cryptographic security, trust anchored in the hardware, lifecycle-aware governance, and scalable anomaly detection.

The medical supply chain is increasingly critical as a multifaceted peril, not least because of counterfeiting, damaging updates, and lack of regulation that endangers patients and makes institutions vulnerable. Here, blockchain technologies emerged as a suitable tool that could enhance the visibility, auditability, and trust in distributed healthcare systems for better transparency, traceability, and trust in the disjoined healthcare systems.

The dialogue on penetration testing pointed out the lack of robust frameworks capable of simulating sophisticated, real-life sieges on IoMT devices. To capture IoMT device security in the real-world context, novel modular, automated, and AI-driven penetration testing frameworks need to be integrated because conventional security evaluations fall short. This approach not only strengthens the technical firewall, but also meets regulatory standards like HIPAA and GDPR, thereby safeguarding sensitive health data.

This work describes the need for a focused exploration of lightweight and flexible security designs that address the needs of implantable and wearable devices, which are constrained by limited resources.

Improving blockchain scalability and interoperability is critical for dealing with large, real-time streams of healthcare data, while penetration testing frameworks need to evolve into continuous, self-learning frameworks able to autonomously identify and mitigate risks. Fostering interdisciplinary collaboration between medical doctors, engineers, lawmakers, and specialists in cybersecurity will be important for developing common international benchmarks that ensure appropriate levels of safety and clinical usefulness and ease of use.

As a matter of fact, to defend the Internet of Medical Things, the problem cannot be approached as purely a technological challenge; rather, it is a clinical imperative. On the other hand, the healthcare industry can establish a digital ecosystem that supports the evolution of medical technologies without endangering the safety and privacy of the patients by enhancing the protective cryptographic barriers, transparency in the supply chains, and advanced penetration testing.

6. Acknowledgement

The author would like to thank and express appreciation to Mr. Kanishka Yapa, lecturer in charge, and Mrs. Helani Herath, instructor, for their guidance, support, and useful suggestions through their instruction during the entire period of this study. The author would like to express his appreciation to the Sri Lanka Institute of Information Technology (SLIIT) for creating an enriching scholarly atmosphere and for providing the relevant resources for the study. The author would also like to express their appreciation to the author's family and friends for their support and guidance which immensely helped in the author's work towards the research paper.

7. Author Information

Pasan Thedasara Jayarathna is pursuing a bachelor's degree in Cybersecurity and Information Assurance at the Sri Lanka Institute of Information Technology. His research on the Internet of Medical Things (IoMT) tackles issues related to security risks, testing methodologies, and the application of blockchain technology in the healthcare supply chain. His academic work on the design of secure software, automated testing, and digital forensics gave him a thorough grasp of the practical components of cybersecurity. Professionally, he aims to merge artificial intelligence, blockchain technology, and zero-trust models into dynamically secure and resilient healthcare systems.

8. Basic format for journals:

[1] A. Musamih et al., "A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain," in IEEE Access, vol. 9, pp. 9728-9743, 2021, doi: 10.1109/ACCESS.2021.3049920.

[2] A. G. Jaafar et al., "A Raise of Security Concern in IoT Devices: Measuring IoT Security Through Penetration Testing Framework," in International Journal of Advanced Computer Science and Applications, vol. 15, no. 5, pp. 676-690, 2024, doi: 10.14569/IJACSA.2024.0150568.

[3] F. M. A. Khan et al., "Advancing IIoT with Over-the-Air Federated Learning: The Role of Iterative Magnitude Pruning," arXiv preprint arXiv:2403.14120, 2024.

[4] X. Sha et al., "An Explicable Keystroke Recognition Algorithm for Customizable Ring-Type Keyboards," in IEEE Access, vol. 8, pp. 22933-22944, 2020, doi: 10.1109/ACCESS.2020.2968495.

[5] I. A. Omar et al., "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," in IEEE Access, vol. 9, pp. 37397-37409, 2021, doi: 10.1109/ACCESS.2021.3062471.

[6] W. Alkhader et al., "Blockchain-Based Decentralized Digital Manufacturing and Supply for COVID-19 Medical Devices and Supplies," in IEEE Access, vol. 9, pp. 137923-137940, 2021, doi: 10.1109/ACCESS.2021.3118085.

[7] T. Haigh and C. Landwehr, "Building Code for Medical Device Software Security," IEEE Cybersecurity Initiative, Tech. Rep., 2015. [Online]. Available: https://ieeecs-

media.computer.org/media/technical-activities/CYBSI/docs/BCMDSS.pdf

[8] Heterogeneous Integration Roadmap Technical Working Group, "Chapter 19: Cyber Security," in Heterogeneous Integration Roadmap, 2021 Edition, IEEE Electronics Packaging Society, 2021. [Online]. Available: https://eps.ieee.org/images/files/HIR_2021/ch19_security1.pdf

[9] "Securing Medical Wearables from Supply Chain Threats," *HealthManagement.org*, vol. 25, no. 3, pp. 1–2, 2025. [Online]. Available: https://healthmanagement.org/c/imaging/issuearticle/securing-medical-wearables-from-supply-chain-threats.

[10] G. Chu *et al.*, "Penetration Testing for Securing IoT-Enabled Healthcare Systems: A Focus on Wearable Devices and Remote Surgery," in *Proc. 2024 IEEE Int. Conf. Bioinformatics Biomedicine (BIBM)*, Lisbon, Portugal, 2024, pp. 5944–5951, doi: 10.1109/BIBM62325.2024.10822619.

[11] A. Goswami *et al.*, "Prevention and Mitigation of Disruptions in Medical Device Supply Chains: A Policy Perspective," *J. Sci. Policy Governance*, vol. 24, no. 1, pp. 1–20, Apr. 2024, doi: 10.38126/JSPG240108.

[12] Q. Zhang *et al.*, "OTA-Key: Over the Air Key Management for Flexible and Reliable IoT Device Provision," arXiv:2412.11564 [cs.CR], Dec. 2024.

[13] X. Feng *et al.*, "Detecting Vulnerability on IoT Device Firmware: A Survey," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 1, pp. 25–41, Jan. 2023, doi: 10.1109/JAS.2022.105860.

[14] A. Saini *et al.*, "Multi-MedChain: Multi-Party Multi-Blockchain Medical Supply Chain Management System," in *Proc. 2024 IEEE Annu. Congr. Artif. Intell. Things (AIoT)*, Gold Coast, Australia, 2024, pp. 153–159, doi: 10.1109/AIoT63253.2024.00038.

[15] M. A. Almaiah *et al.*, "Security Risk and Breach Detection Approach Based Blockchain for Medical Applications," *IEEE Access*, vol. 12, pp. 171876–171896, 2024, doi: 10.1109/ACCESS.2024.3487217.

[16] Y. Sun *et al.*, "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.