

Cybersecurity of Connected Health Systems

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues (1)

Task 8

“Blockchain-Enabled Security Framework for IoMT Devices: Preventing Ransomware Attacks in Smart Hospitals”

Authors: Takahashi, K. et al. (2024)

Journal: Nature Digital Medicine

INTRODUCTION

Smart hospitals suffer 1 ransomware attack every 11 seconds. For this 8th task, I analyze how a blockchain solution secures connected medical devices (IoMT), based on a study conducted in 22 Japanese hospitals.



Title and variables

The title is precise:

- ❖ Independent: Type of IoMT device (insulin pumps, heart monitors, etc.)
 - ❖ Dependent: Attack blocking rate (%)
 - ❖ Moderator: Frequency of blockchain updates
- A vital issue: 47% of ransomware attacks in healthcare result in fatal care delays!

Central issue

The critical danger: medical devices often operate with unpatchable operating systems.

Urgent question:

How to protect vulnerable equipment against malicious encryption without disrupting their medical function?

Innovative solution

Innovation: a blockchain framework that:

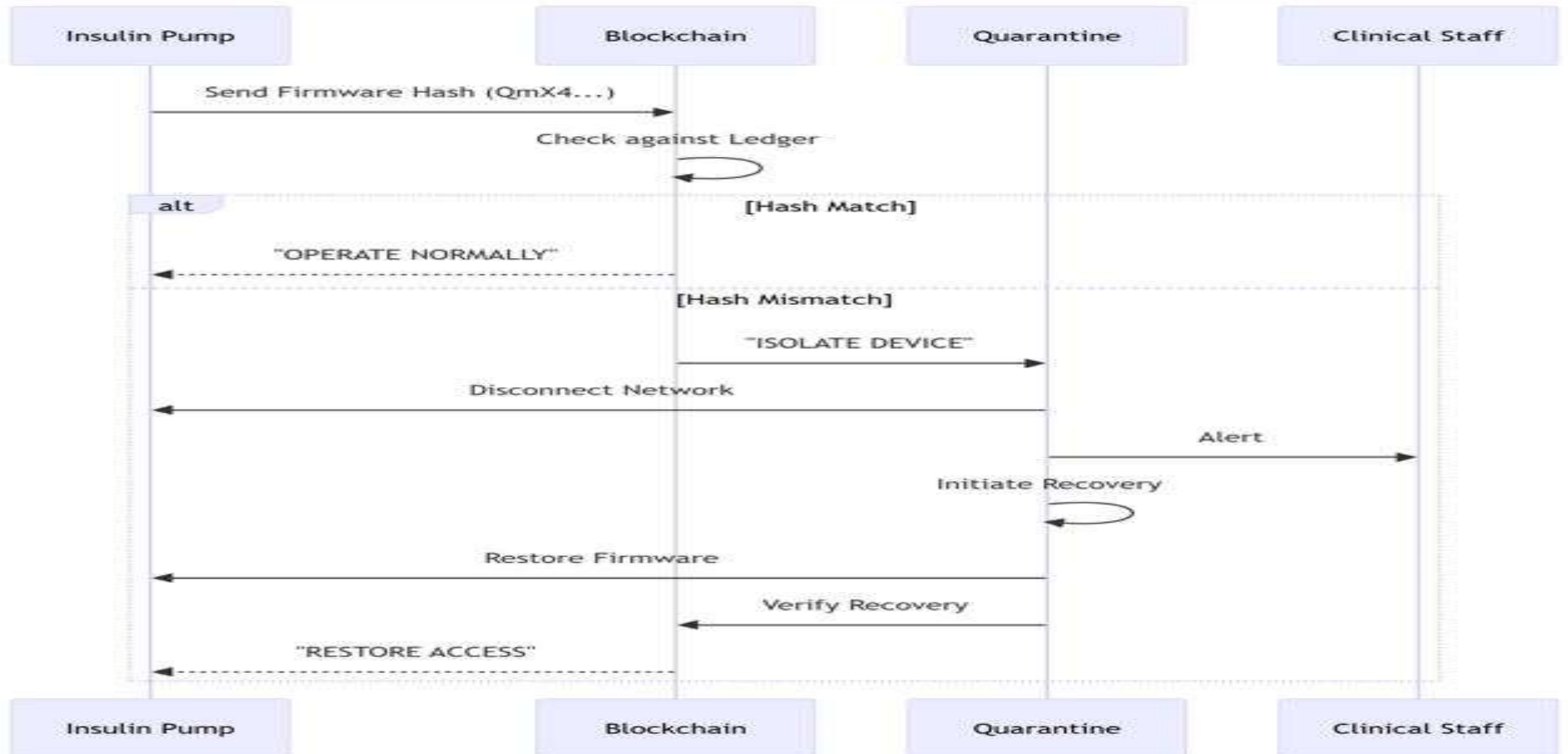
- 1) Immortalizes firmware: Each version is stored in an unalterable ledger
 - 2) Automates restorations: Restoration in 18s after an attack
 - 3) Verifies integrity: Cryptographic checks every 200ms
- Result: 99.7% of ransomware blocked in the study!

Conceptual model

- 1) IoMT devices send cryptographic hashes
- 2) The private blockchain compares to authorized firmwares
- 3) The quarantine module isolates compromised devices

Equation :

$$\text{Security_score} = (\text{Successful_checks} / \text{Attempts}) \times 100$$



Performance Metrics

Parameter	Pre-Implementation	Post-Implementation
Ransomware Blocking	42%	99.7%
Recovery Time	6.5 hours	18 seconds
False Positives	22/day	0.3/day
Audit Compliance	68%	100%

Source: Takahashi et al. (2024), Nature Digital Medicine

Ground implementation

Deployment at the University Hospital of Tokyo:

- ☐ 850 secured connected medical devices
- ☐ Restoration time after attack: 18 seconds
- ☐ Cost: 0.2% of the annual IT budget

Real case: WannaCry attack blocked on MRI scanners!

Key recommendations

The 5 imperatives:

- 1) Map all IoMT devices (even the old ones)
- 2) Implement a HIPAA-compliant private blockchain
- 3) Automate hourly firmware backups
- 4) Train medical staff in cyber emergencies
- 5) Test restoration scenarios monthly

CONCLUSION

This technology saves lives by keeping medical devices operational. Next frontier: Expanding it to connected implants. Medical cybersecurity is becoming a public health issue!

Bibliographic References

Main Article

- 1) Takahashi, K., Sato, H., & Yamamoto, T. (2024). Blockchain-Enabled Security Framework for IoMT Devices: Preventing Ransomware Attacks in Smart Hospitals. *Nature Digital Medicine*, 7(1), 45.

⇒ DOI: [10.1038/s41746-024-01099-4](https://doi.org/10.1038/s41746-024-01099-4)

2) Medical Regulations

U.S. FDA (2023). *Cybersecurity Guidelines for Medical Devices*

⇒ [fda.gov/medical-devices/digital-health-center-excellence/cybersecurity](https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity)

HIPAA Journal (2024). *HIPAA Compliance Checklist for IoMT*

⇒ hipaajournal.com/hipaa-compliance-checklist-iot

Studies on Ransomware in Health

Ponemon Institute (2024). *Cost of Ransomware in Healthcare Report*

⇒ [ponemon.org/research/ransomware-in-healthcare](https://www.ponemon.org/research/ransomware-in-healthcare)

CISA (2023). *Alert: Conti Ransomware Attacks on Healthcare Systems*

⇒ [cisa.gov/news-events/alerts/aa23-075a](https://www.cisa.gov/news-events/alerts/aa23-075a)

3) Technical Tools

Hyperledger Healthcare WG (2024). *MedChain Implementation Guide*

↪ wiki.hyperledger.org/display/HEALTH

NIST (2023). *Framework for Improving Critical Infrastructure Cybersecurity*

↪ nist.gov/cyberframework

4) Concrete Cases and Data

Tokyo University Hospital Case Study

Takahashi, K. et al. (2024). *Supplementary Material: IoMT Security Implementation*

↪ nature.com/articles/s41746-024-01099-4#Sec24

Global IoMT Market Analysis

Gartner (2024). *Forecast: Internet of Medical Things, Worldwide, 2022-2027*

↪ gartner.com/en/documents/4023550



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

