Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-269-2_11

Chapter 11: Healthcare IoT Security: From Vulnerabilities to Trustworthy Systems

Afef Kchaou [1,2], Hatem Garrab [3,4]

[1] *IUT Bordeaux, 15 Street of Naudet, 33170 Gradignan, France.*
[2] *Tunis El Manar University, Sciences Faculty of Tunis, 20 Street of Tolède, 2092 Tunis, Tunisia.*
[3] *Electronics and Micro-Electronic Laboratory (LEμE), Bd de l'environnement, Monastir 5000, Tunisia.*
[4] *Higher Institute of Applied Sciences and Technology of Sousse, University of Sousse, Street Taher Ben Achour, 4003 Sousse, Tunisia.*

Abstract: New generation of connected healthcare systems has emerging digital technologies and medical science. They are converging more and more with time. This development delivers healthcare: it connects smart medical devices, analysis real-time data, and executes the make an advanced clinical decision. This progress creates more attached, efficient, and patient-centered healthcare ecosystem. With recent advancements in Internet of Things (IoT), continuous monitoring became possible. As well as predictive analytics and patient-centered care. On the other hand, with possible injury directly implicating patient safety and trust, growing requirement on Health-IoT (H-IoT) has carried critical security and privacy concerns. This chapter presents a brief overview of the H-IoT applied-systems. Device classification and architectural layers are also described. As well, fundamental security challenges are including: weak authentication, data integrity risks, and supply chain vulnerabilities. Then, real-world incidents and attacks in a infusion pump is discussed, following by an example of pacemaker recalls. Indeed, regulatory and ethical dimensions of H-IoT are discussed. Additionally, this chapter a survey reveals emerging solutions, such as blockchain, lightweight cryptography, zero-trust architectures, and privacy-preserving analytics and post-quantum security. Finally, this chapter concludes by some future oriented new IoT healthcare security.

Keywords: Healthcare IoT (H-IoT), Cybersecurity, Medical Devices, Privacy, Cryptography, Patient Safety.

1 Introduction

Over the last two decades, the health domain has seen a paradigm shift due to the merger of medical science with digital innovation. The principal phenomena announced into clinical practice are the Internet of Things (IoT), which actually has emerged as one of the most transformative forces, and offered a new opportunity to the concept of

Healthcare IoT (H-IoT). This combined system can merge wearable sensors, implantable devices, in-hospital systems, and home-based monitoring platforms for the real-time observation of patients. As we well this ecosystem performs predictive analytics, and clinically making decisions based on data.

At the moment, a smart ECG patch can continuously display a cardiac patient by recording cardiac activity and securely transmits the data to cloud servers for researcher review (Page et al., 2015). Glucose monitor systems for diabetic patients give real-time alerts and have the possibility to expand capabilities through integrations with insulin pumps, which regulate automate glucose injection. In hospitals and clinics, infusion pumps, ventilators, and MRI scanners are progressively being linked to electronic health registers. It delivers an easy access to a centralized console which is a practical tool for clinicians and patricians (Desai et al., 2025). This kind of innovations continue the promise of passing improvement in many features of modern medicine.

The kind of object connectivity opens an important risk. The medical data is among the most searching types of private and confidential information. Yet, it may result in irreparable risk for patients. Hospitals remain a target for ransomware and service attacks, where constrained devices are often unable to support robust cryptography. (Gadde et al., 2023). In extreme cases, vulnerabilities within life-supporting devices, like pacemakers or insulin pumps, pose direct harm to the lives of patients.

This chapter will address the challenge for the security of Healthcare IoT. Section 2, we start by giving a general overview of the H-IoT eco-system. We specify categories of devices, architectural layers, and participant dynamics. Section 3, we discuss the key security challenges, while in Section 4, examples of real-world incidents will be discussed. Section 5, we present regulatory and ethical frameworks, with a particular focus on compliance and responsibility. Section 6, we will focus in presenting some of the developing solutions to ensure confidential data and reinforce the security. We include here, the utilization of blockchain, the lightweight cryptography, the zero-trust approaches, and the post-quantum security, as an emerging example. Section 7 we will conclude with general considerations to preserve not only patient confidentiality but also public trust in digital medicine as new alternative in the near future.

2. The Healthcare IoT Ecosystem

IoT in healthcare is a homogeneous system that dynamically interacting ecosystem of devices, networks, applications, and stakeholders. Its complexity arises in device diversity which play an important role to deliver patient care. Understanding this novel system is crucial to appreciate both the scale of invention involved and the scope of security challenges.

2.1 Classes of IoT Healthcare devices.

H-IoT device can be categorized into four major groups, as depicted in Fig. 11.1. Each category possesses different advantages and security threats (Bradhan et al. 2024).

Big public wearables devices, e.g. Apple Watch, Fitbit trackers, and Bluetooth glucose monitors, make real-time physiological data accessible immediately. They are often designed using insecure wireless protocols, vulnerable mobile applications, and weak encryption, making them susceptible to data hacking. Implantable medical devices, e.g. pacemakers, insulin pumps, and neuro-stimulators, interact directly with the human body, where their reliability and security are a critical issue. However, due to the difficult inaccessibility after commercialization, updates are problematic, while wireless services often allow for remote, potentially serious exploitation. In hospitals and clinical, connected objects and devices such as MRI scanners, infusion pumps, and robotics surgery platforms are directly connected into the electronic health record environment to simplify care. However, the attack surface for cyber intrusions is done on out-of-date and the unpatched operating systems is significantly expand.

Developed systems for the home healthcare include remote monitoring kits and telehealth suites, can now enable patient's surveillance and expand care beyond clinical settings. However, these systems regularly depend on high utilization of Wi-Fi access as well as the spectrum, without specialized inaccuracy, and physical interfering is also shared. While it has significant serious security compromises, connectivity and convenience continue common hunts in the H-IoT across all these categories.

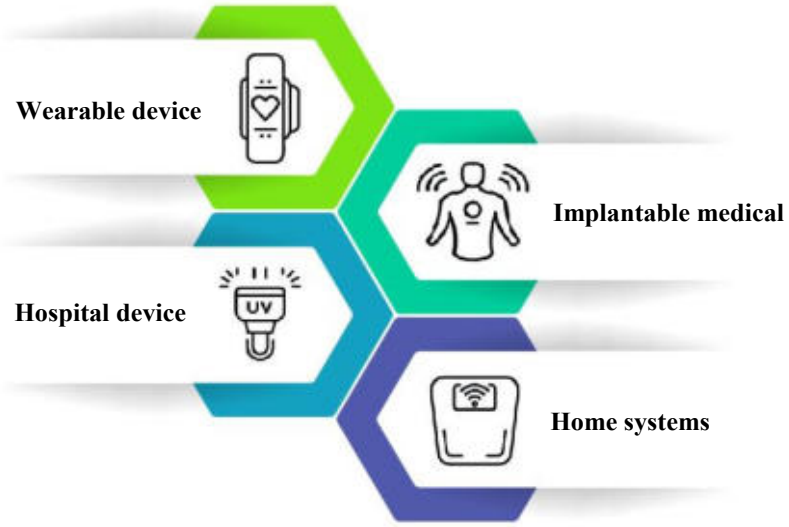

Fig. 11.1 Healthcare IoT categories.

2.2 H-IoT Data Flow Architecture

Compared to conventional systems, healthcare IoT architecture can be conceptualized in several layers. Fig. 11.2, shows and gives an overview in each of which IoT can be used (Alaba et al., 2024).

Analyzing the figure, the perception layer comprises sensors, devices, physiological data collection, e.g. such as heart rate, temperature, or motion. Most of these devices have a limited power processors and memory size. Consequently, advanced security tools pose problem and difficulty to implement them. Protocols such as BLE, Zig-bee, Wi-Fi, LTE, or 5G in the network layer need to be secured through the communication of data. In more details, each communication technology has their advantages and disadvantages in terms of security. For example, older Bluetooth versions are easy to eavesdropping and repeat attacks. The processing layer takes data accumulations by means of cloud or edge computing infrastructures. Also cloud-based solutions offer scalability but make sensitive information vulnerable to misconfigured servers, insider threats, and data openings. As well, edge computing permits for improved privacy and lesser latency, but, it unlocks up nodes to different vulnerabilities. Finally, the application layer provides an interface for clinicians, patients, and other insurer. While many applications provide fundamental functionalities like alerts and dashboards, the weakness of mobile or web interfaces security leads to unauthorized access and data escapes.

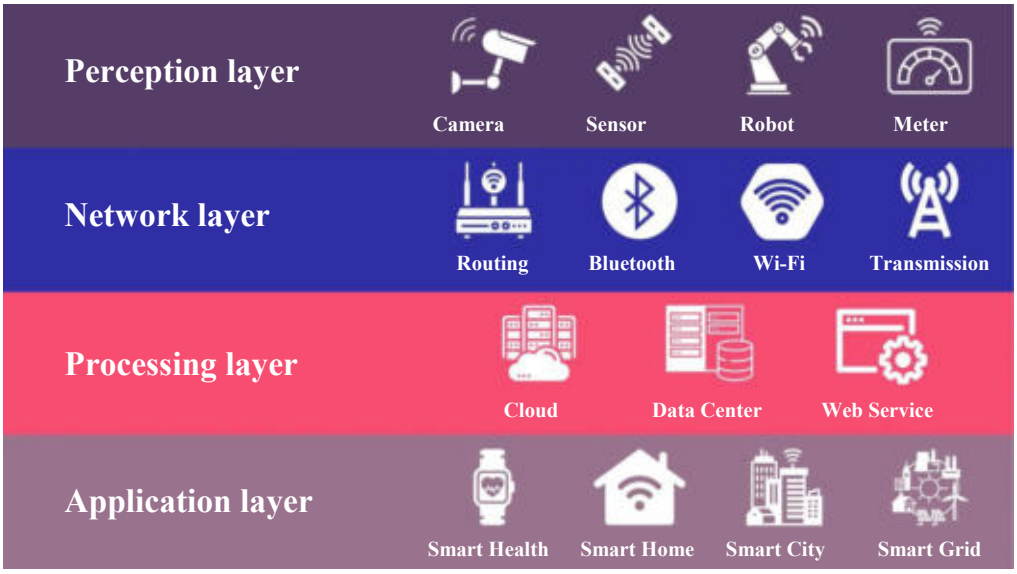

Fig. 11.2 Different application of Internet of Things (IoT).

2.3 Stakeholders in the Ecosystem

The security of healthcare IoT is influenced by the technology progress and by the complex web of stake-holders with conflicting priorities. Device safety and data protection have an important depend on patient's utilization and access. This latter is responsible for managing and securing clinical networks and his healthcare provides. Also, manufacturers should assure the balance cost and development timelines with security needs. As well, researchers through regulators enforce safety and privacy standards to insure and rely on data for analytics and innovation. For example, manufacturers may reduce safeguards to meet cost or delivery targets, leaving hospitals and patients exposed despite regulatory safeguards. As a result, these competing interests often inhibit consistent security practices.

3. Key Security Challenges

Nowadays, security becomes the most critical enabler for H-IoT. Serious security threats and features like universal connectivity, distributed architectures, and patient data-center collection, make H-IoT a transformative field to expose it. Unlike ordinary IoT devices, failures in the health domain can expose life to death consequences. An access to devices and lose control may compromise patient privacy, disrupt operations within the hospital, or may directly cause loss of lives and a disease (Somasundaram et al., 2021; Kumar et al., 2023).

The key challenge begins with data privacy and confidentiality, as illustrated in Fig. 11.3. Medical data is characteristically sensitive and irreversible once exposed. Commonly, health patient-data is diffused over insecure wireless networks and often accessible for public. Also, these data are stored on a low-cost and unprotected cloud server. By blocking malicious attackers or insiders, the authentication/access control process remains vulnerable and fragile. With many devices operating on virtual licenses leading to privilege and threatening the entire communication networks.

Data integrity remains a critical concern. Like many systems still lack tamper-proof and protections such as digital signatures or blockchain-based audit logs. At the device level, imposing manufacturers to compromise on security features is primordial constraints, especially in hardware and power.

In year 2017, the U.S. Food and Drug Administration (FDA) have recalled nearly half a million pacemakers found to be vulnerable to remote exploitation. The identified problem was very dangerous and has leading to a partial or complete loss of control. However, a technical limitation can result an unsafe device operation: a diminution trust in hardware reliability, and, in some cases, an inability to update firmware. The potential

consequences are multiples. For example, data received from the sensor can be manipulated, leading to falsified ECG readings, and could affect patient's life.

A major feebleness is network security where wireless connections make it easier for hackers to spy on data. As well as launch man-in-the-middle attacks, or disrupt systems through DDoS attacks. Mirai botnet incident was clearly shown, which could easily target hospital or clinic networks. The problem is exacerbated by the poor compatibility between devices. Hospitals often connect equipment salted by different companies, each with its proper security standards. If one device is uncertainly protected, it can become an open gate for attackers to penetrate into the hole system.

Because of scalability and management, fixing these issues become a hard challenge. In real, most hospitals can't manually update or monitor tens of thousands of connected machines. Some advanced solutions exist, for example, automated systems can remote updates over-the-air and manage devices. Yet, these technologies are still very costly and not accessible everywhere. As a result, many hospitals, especially those with limited budgets, can't have enough money. So, leaving their systems un-updated make them more vulnerable to attacks.

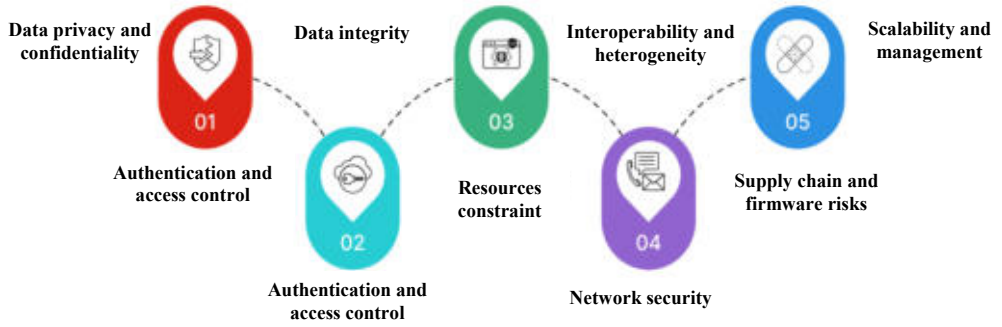

Fig. 11.1 H-IoT security chain challenges.

4. Case Studies and Incidents

Whereas the theoretical analysis of vulnerabilities is quite useful, only through actual incidents we can analysis the real weight of challenges with healthcare IoT security. Many high-profile cases in the last two decades have been recorded in how the overwhelming consequences of weak defences can range from disturbed hospital operations to serious risks for patients. These critical case studies emphasize the urgency in securing H-IoT systems. They form experiment lessons for both legislators and technology developers to enhance their researcher and studies.

4.1 WannaCry Ransomware Attack

In May of 2017, WannaCry ransomware attack spread across the globe, infecting hundreds of thousands of systems in more than 150 countries, recoding as the first attack in history of world hospital service. Among the hardest-hit victims was the United Kingdom's National Health Service (NHS) (Ghafur et al., 2019).

Damage are seriously, information system is affected and brought chaos to the delivery of care. Within few hours, hospital computers and encrypted medical devices forcing staff to cancel > 19,000 appointments and rerouted emergency patients to modest services. Also, ambulances were redirected and operating rooms are temporarily closed.

This attack was a reason of old and unpatched versions of Windows systems that were deeply installed into a great deal of hospital infrastructures. The medical devices were not attacked but rather to exploit the outdated. This incident underlined two important realities: (1) The use of outdated systems creates disproportionate vulnerabilities for healthcare providers. (2) Beyond financial loss, disruption of critical care from ransomware extends (Tully et al., 2020).

4.2 Pacemaker Recall

In the same year (2017), the FDA ordered the recall > 500,000 pacemakers from St. Jude Medical® company. Researchers had discovered and demonstrated that the devices could be remotely hacked and could potentially be fatal. This default leads to a failure by altering pacing or delivering inappropriate shocks (Zhang et al., 2015). Different to classical software patches delivered and support by company for consumer devices, these vulnerabilities need a firmware update, a task note easy to deliver in a clinical setting which creates logistical and ethical problems.

This huge recall of pacemakers underlines the atypical challenge of securing implantable devices. Different from smartphones, tabs, or laptops, which consumers can easily replace, most of medical implants are invasive and usually integrated inside patients for many years. It is important to mention and cite the work given by (Ghafur et al. 2019) in this context. Their results produce a narrow window for remediation, with any medical intervention carrying risks.

4.3 Insulin Pump Exploits

A widely used system by diabetic patients have also been shown vulnerable to cyber-attacks: The insulin pumps. It is wireless communication protocols were found unsupported strong encryption and thus in many pump designs (Voelker et al., 2019).

However, an attacker can therefore capture the signals and change insulin dosages. In one proof-of-concept demonstration, engineering has showed that is potentially possible to deliver wrong and deadly doses by exploiting weak authentication.

In a real-world setting and though no large-scale attacks, experiences have been performed. The demonstrations shown how life-sustaining devices can be weaponized if missing unprotected. As well, researchers have underlined the ethical obligation of the manufacturers to balance usability with robust defenses. It give devices a level of security when they are deployed outside of clinical supervision, like home environments or work conditions (Stergiopoulos et al., 2023).

4.4 MRI, Infusion Pump Vulnerabilities.

In recent years, exactly in 2020, vulnerabilities were reportedly exposed by cybersecurity companies in MRI machines, infusion pumps, and other hospital-based devices. However, most of such systems entered on out-dated operating systems and stilled unpatched out of concern that software updates. Consequently, it could be negatively disrupting clinical workflows or void regulatory approvals. Engineering and developers demonstrate how attackers could distantly remote parameters of infusion pumps to alter medication dosages or use MRI scanners as entry points into hospital networks (Badrouchi et al., 2020).

These incidents showed that the risks of H-IoT were general. Even where individual devices did not straight pose safety risks to patients, but they could be used as access points to more dangerous attacks. Since of the interconnected nature of modern hospitals, a single vulnerable device could be used to remote whole clinical ecosystems.

5. Regulatory and Ethical Considerations

Keeping IoT systems safe in healthcare is a big technical challenge, but it’s also guided by laws and ethics. Important rules like HIPAA in the U.S.A., GDPR in Europe, and standards from the FDA and ISO set the basic requirements for protecting data, securing devices, and managing risks (Alamri et al., 2022). However, in reality, these rules are not always well enforced, (especially for small companies or those working across global supply chains), making it hard to keep security strong everywhere.

6. Emerging Technical Solutions and Future Directions

Experts and developers are always searching for new solutions those combine cryptography with artificial intelligence and new generation networks. However, securing healthcare IoT is a difficult task. In this section, we present the promising new directions making connected healthcare more secure and safe.

6.1 Blockchain and Distributed Ledger Technologies

The advantage of blockchain in H-IoT can be viewed in the light of providing immutable, decentralized record-keeping that may enhance data integrity and accountability, according to (Deshpande et al. 2017). For the moment, the MIT MedRec project illustrates how Ethereum-based ledgers can provide for patients more control degree over health records/registers, while guaranteeing auditable access logs. Nonetheless, there are many issues to be fixed such as scalability and energy efficiency.

6.2 Symmetric Lightweight Cryptography

Resource-constrained healthcare IoT devices, such as wearables and implantables, cannot always support standard implementations of conventional algorithms, such as AES. To resolve this, lightweight symmetric ciphers have been developed for resource-constrained environments (McKay et al. 2016). Such algorithms come with reduced memory, power, and GE requirements, yet are adequate for confidentiality and integrity.

- **PRESENT:** A 64-bit block cipher with 80/128-bit keys, optimized for hardware efficiency. It is one of the most compact designs; it requires only ~1570 GE and is highly suitable for implantable devices.
- **SIMON and SPECK:** Families of block ciphers designed by NSA for hardware and software efficiency, respectively. For example, SIMON-128/128 has ~878 GE in hardware, which provides one of the smallest footprints among recent ciphers.
- **ChaCha20:** A stream cipher optimised for software performance, especially the ARM processors common in medical devices. Unlike AES, which enjoys hardware acceleration, ChaCha20 shines on low-cost platforms without cryptographic coprocessors.

Table 11.1 Performance characteristics for lightweight ciphers on representative medical device platforms. Lightweight ciphers such as these enable even battery-powered, always-on medical devices to implement secure communications with acceptable overheads. However, the selection of an algorithm for usage has to balance

efficiency with resistance to cryptanalysis because lightweight designs usually reduce complexity at the expense of long-term robustness (Tsantikidou et al., 2022).

Table 11.1 Performance characteristics of lightweight ciphers.

Algorithm	Block size	Key size	HW (GE)	Energy (μW)	Throughput (Mbps)
AES-128	28	128	3400	9.5	142
Present	64	80/128	1570	2.1	200
Simon-64/96	64	96	878	1.8	176
ChaCha20	Strem	256	N/A*	3.2	312

*ChaCha20 is optimized for software implementation

6.3 Lightweight Elliptic Curve Cryptography (ECC)

While symmetric algorithms provide confidentiality and integrity, Healthcare IoT also needs public-key mechanisms for secure key establishment, authentication, and digital signatures. Traditional algorithms like RSA are not practical in constrained devices due to large key sizes and extensive computation. On the other hand, ECC provides equivalent security with much smaller keys, thus yielding the best security-to-performance ratio in resource-limited environments (Lara-Niño et al., 2018). Table 11.2 summarizes elliptic curves and implementation optimizations that can be used for Healthcare IoT devices.

Table 11.2 ECC curve options and optimizations for H-IoT.

Category	Option	Key Benefit	Limitation
Curves	NIST P-256	Standardized, widely supported	Heavy for constrained devices
	Curve25519	Fast, secure, side-channel resistant	Limited legacy support
	secp256k1	Optimized for verification	Less suited for signing
Optimizations	Fixed-base mult.	60–80% faster ops	Needs extra memory
	Montgomery ladder	Side-channel resistant	Slightly slower
	Sliding window	Fewer additions	Risk of leakage if careless

In particular, ECC is relevant for implantable and wearable devices that need to pair securely with external readers, physicians' consoles, or cloud servers. When combined

with lightweight symmetric ciphers for session encryption, ECC enables hybrid cryptographic protocols that effectively balance efficiency and robust security throughout the H-IoT ecosystem.

6.4 AI and Machine Learning for Security

Artificial intelligence can now be used to detect abnormal traffic and device behavioral patterns. Machine learning algorithms will help in distinguishing between legitimate and malicious activity, thus enabling real-time intrusion detection in the hospital networks. Panesar et al. (2019), Nankya et al. (2024), and Tilala et al. (2024) demonstrate applications of machine learning in anomaly detection for infusion pumps and ventilators in some pilot studies conducted at Johns Hopkins. Yet AI itself is introducing risks in terms of adversarial attacks, where malicious actors manipulate input data to bypass defenses.

6.5 Zero-Trust Architecture

Zero-trust security, often summed up by the idea: never trust, always verify, and is becoming more common in healthcare (Tyler et al., 2021). Actually, this technique improves the security of healthcare IoT in many systems. The principle of its operation is as the following: (1) checking user identities, (2) dividing networks into smaller secure units, and (3) allowing each user or device access only to what they really need. These three actions make it much harder for hackers to enter into a system.

However, setting up a zero-trust system is not easy. It requires major changes to the existing network and a lot of financial investment. For many hospitals and healthcare organizations that already have limited budgets, putting these measures in place can be a serious challenge.

6.6 Secure Lifecycle Management of an H-IoT Device.

According to reference (Sodhro et al. 2018), security in Health-IoT devices requires more attention. From support to critical design, it includes:

- Design: Hardware roots of trust, secure coding practices.
- Deployment: Secure provision of cryptographic keys.
- Operation: Regular OTA firmware updates and monitoring.
- Withdrawing: Secure distributing and removal of devices.

As a recommendation, FDA now explicitly advice manufacturers to define a lifecycle security strategy.

6.7 Data analytics with privacy protection.

Health care nowadays relies much on data aggregation, while privacy concerns increasingly raise a barrier to data sharing. Among various solutions, privacy-preserving methods (Sharma et al., 2018) include federated learning, homomorphic encryption, and differential privacy. These approaches enable training predictive models without leakage of raw patient data, thus balancing medical progress against confidentiality.

6.8 Security of Edge and Fog computing.

Edge and fog computing lower dependence on a central cloud server by processing data closer to its source. It improves latency, provides reliability, and reduces the attack surface. Hospital ICUs use edge-based analytics to monitor patients with acute conditions in real time. However, the protection needs of an edge node are also high because they often become attractive targets of attacks (Dush et al., 2019).

6.9 Post-Quantum Cryptography

Looking ahead, quantum computing will eventually break widely deployed algorithms like RSA and ECC. For devices intended to operate for at least tens of years, this creates an existential security risk. Lattice-based and code-based post-quantum cryptographic algorithms have been and are being standardized to ensure resistance against future quantum attacks. The integration of such algorithms into H-IoT devices today may provide the required security for operation in decades to come (SaberiKamarposhti et al. 2024).

Conclusion

IoT in healthcare applications has become essential to modern medicine. It offers many advantages, such as, continuous monitoring, personalized treatment, and evidence-based healthcare transfer. Nevertheless, the identical interconnectedness that fuels these benefits causes a complex mesh of vulnerabilities.

To keep healthcare IoT correctly safe, a complete approach is needed. New technologies such as blockchain, lightweight cryptography, zero-trust systems, and federated learning can do it.

References

Alaba, F. A. (2024). Iot architecture layers. In *Internet of Things: A Case Study in Africa* (pp. 65-85). Cham: Springer Nature Switzerland.

Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health IoT. Sensors, 23(1), 218.

Badrouchi, F., Aymond, A., Haerinia, M., Badrouchi, S., Selvaraj, D. F., Tavakolian, K., ... & Eswaran, S. (2020). Cybersecurity vulnerabilities in biomedical devices: A hierarchical layered framework. Internet of Things Use Cases for the Healthcare Industry, 157-184.

Dash, S., Biswas, S., Banerjee, D., & Rahman, A. U. (2019). Edge and fog computing in healthcare–A review. Scalable Computing: Practice and Experience, 20(2), 191-206.

Desai, V., Sule, A., Mishra, R., Jadhav, V., Sayyad, J., & Shukla, M. (2025, May). Networked Hospitals: An Approach for Scalable Healthcare Network Infrastructure with Security Protocols. In 2025 7th International Conference on Energy, Power and Environment (ICEPE) (pp. 1-6). IEEE.

Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report The British Standards Institution (BSI), 40(40), 1-34.

Gadde, S., Amutharaj, J., & Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. Journal of Information Security and Applications, 73, 103412.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ digital medicine, 2(1), 98.

Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. H., & Hosen, A. S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. Electronics, 12(9), 2050.

Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. Ieee Access, 6, 72514-72550.

McKay, K., Bassham, L., Sönmez Turan, M., & Mouha, N. (2016). Report on lightweight cryptography (No. NIST Internal or Interagency Report (NISTIR) 8114 (Draft)). National Institute of Standards and Technology.

Nankya, M., Mugisa, A., Usman, Y., Upadhyay, A., & Chataut, R. (2024). Security and privacy in E-health systems: a review of AI and machine learning techniques. IEEE Access.

Page, A., Kocabas, O., Soyata, T., Aktas, M., & Couderc, J. P. (2015). Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance. Annals of Noninvasive Electrocardiology, 20(4), 328-337.

Panesar, A. (2019). Machine learning and AI for healthcare (Vol. 10). Coventry, UK: Apress.

Pradhan, B., Bhattacharyya, S., & Pal, K. (2021). IoT-based applications in healthcare devices. Journal of healthcare engineering, 2021(1), 6632599.

SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10).

Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing, 22(2), 42-51.

Sodhro, A. H., Pirbhulal, S., & Sangaiah, A. K. (2018). Convergence of IoT and product lifecycle management in medical health care. Future generation computer systems, 86, 380-391.

Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare internet of things. Wireless Networks, 27(8), 5503-5509.

Stergiopoulos, G., Kotzanikolaou, P., Konstantinou, C., & Tsoukalis, A. (2023). Process-aware attacks on medication control of type-i diabetics using infusion pumps. IEEE Systems Journal, 17(2), 1831-1842.

Tilala, M. H., Chenchala, P. K., Choppadandi, A., Kaur, J., Naguri, S., Saoji, R., ... & Tilala, M. (2024). Ethical considerations in the use of artificial intelligence and machine learning in health care: a comprehensive review. Cureus, 16(6).

Tsantikidou, K., & Sklavos, N. (2022). Hardware limitations of lightweight cryptographic designs for IoT in healthcare. Cryptography, 6(3), 45.

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. Health security, 18(3), 228-231.

Tyler, D., & Viana, T. (2021). Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences, 11(16), 7499.

Voelker, R. (2019). Insulin pumps could be hacked. JAMA, 322(5), 393-393.

Zhang, S., Kriza, C., Schaller, S., Kolominsky-Rabas, P. L., & National Leading-Edge Cluster Medical Technologies 'Medical Valley EMN'. (2015). Recalls of cardiac implants in the last decade: what lessons can we learn?. PloS one, 10(5), e0125987.