World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Security and privacy vulnerabilities in IoT-enabled medical devices: Analyzing cleartext data leakage and metadata exposure

Kavya Pathuri *

Independent Researcher, USA.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(03), 1025-1030

Publication history: Received on 30 April 2025; revised on 08 June 2025; accepted on 11 June 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.3.1029

Abstract

The Internet of Things (IoT) revolutionizes healthcare by integrating everyday medical devices into electronic health systems. While these devices offer convenience and improved patient care, they also raise serious privacy concerns. This article evaluates the security and privacy vulnerabilities of commercially available IoT medical devices, specifically analyzing data transmission from four popular devices: Withings Smart Blood Pressure Monitor, Withings Smart Scale, iHealth Ease Wireless Blood Pressure Monitor, and 1byOne Digital Smart Wireless Scale. Network traffic captured through a custom Wi-Fi access point setup reveals that multiple devices transmit sensitive health data in cleartext, even when utilizing encryption protocols like SSL/TLS. Additionally, metadata exposure allows adversaries to infer sensitive user behaviors and medical conditions. A user-friendly monitoring interface that visualizes data flows and alerts users of potential privacy risks is proposed. The evidence underscores the need for stricter security standards and increased transparency in developing medical IoT devices.

Keywords: Medical IoT Devices; Data Privacy; Cleartext Transmission; HIPAA Compliance; Network Security

1. Introduction

The Web of Things (IoT) encompasses numerous gadgets, including clinical IoT gadgets, that connect with the internet to transmit information. These gadgets, frequently utilized in homes and medical clinics, gather delicate wellbeing data that falls under the assurance of the health care coverage Movability and Responsibility Act (HIPAA). HIPAA orders that substances dealing with electronic patient wellbeing data (ePHI) keep up with its privacy, respectability, and accessibility, while shielding against dangers and unapproved revelations.

Regardless of these prerequisites, weaknesses in clinical IoT gadgets uncover touchy client information. Cleartext transmissions, ill-advised encryption practices, and metadata spillage are common issues. In any event, while utilizing SSL/TLS, a few gadgets send e-PHI in decoded treats, URLs, or other shaky channels. Moreover, network traffic investigation can surmise client conduct and touchy data in light of gadget action and IP addresses.

This article evaluates the protection practices of several popular clinical IoT gadgets, including Withings Brilliant Pulse Screen and iHealth Simplicity Remote Circulatory Strain Screen. The evidence reveals far-reaching, clear-text information transmission and unfortunate improvement rehearsals that risk e-PHI. A user interface is also presented to help clients screen and picture gadget information transmissions, bringing issues to light about privacy risks and advancing better transparency. Lastly, the article highlights the need for stricter security guidelines among IoT makers.

* Corresponding author: Kavya Pathuri.

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

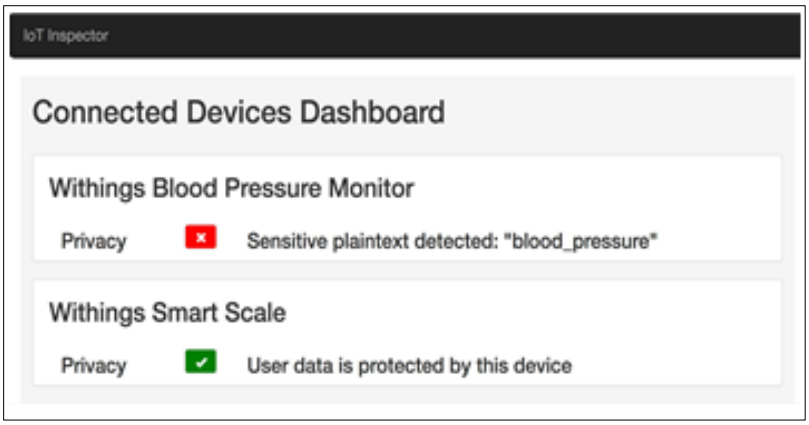

Figure 1 User interface displays connected devices in the home and privacy status

2. Related work

Grouping network traffic as encoded or clear text can be challenging. Cha's technique for recognizing scrambled and decoded traffic involves examining bundle headers and payloads, utilizing tests such as Shannon Entropy and Chi-square. A pattern edge for encryption is laid out by preparing on cleartext (HTTP, FTP) and encoded conventions (SSH, TLS). A connected test recognizes encoded traffic from packed cleartext, as both show high entropy. This article centers around distinguishing uncompressed cleartext from encoded traffic.

While earlier observations on IoT protection weaknesses center mostly around home gadgets, late evidence shows comparable dangers in clinical IoT. For example, the FATS attack recognizes private exercises by dissecting remote traffic, and aloof organization spectators can construe client collaborations from scrambled IoT interchanges. Such weaknesses are especially disturbing for clinical gadgets, where repeating tests like pulse readings create recognizable examples in network traffic.

Dimitrov features the capability of the clinical IoT to upset medical services by smoothing out work processes and further developing information supported care. This article aims to further develop gadget the board and investigation by giving a dashboard to screen continuous clinical gadget traffic and recognize protection gambles.

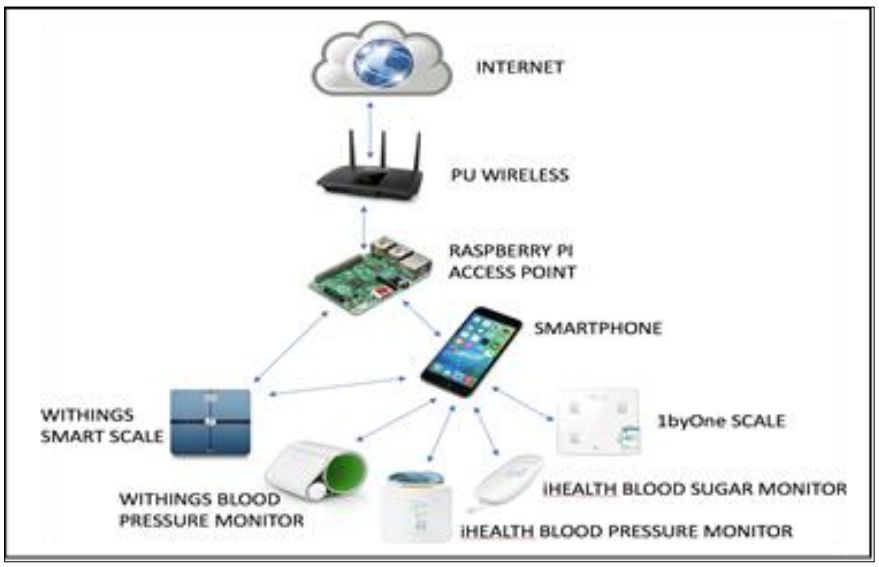

Figure 2 Data collection environment and connection patterns between devices and infrastructure components

Approach	Precision	%packets
cleartext		
Naive ASCII	1	0.5
Shannon Entropy	0.26	16.2

Figure 3 Comparison of cleartext detection approaches on 225,000 packet payloads from the devices studied. The precision metric indicates the prob- ability that a particular approach correctly identifies a payload as cleartext. Column 3 indicates what percent of total packets were identified as cleartext. Less selective approaches identify more cleartext packets, resulting in higher false positive rates

3. Device assessment methods

The protection weaknesses in clinical IoT gadget network traffic was assessed utilizing a three-stage process:

- Data Collection: A Raspberry Pi was set up as a Wi-Fi passageway (AP) to gather traffic from IoT gadgets.
- Clear-text Identification: Caught traffic was examined to recognize decoded wellbeing information.
- Metadata Analysis: Device movement was examined to induce client conduct.
    - Data Collection A Raspberry Pi 3 was designed as a Wi-Fi AP to catch traffic from four clinical IoT gadgets: two pulse screens and two brilliant scales. The traffic was captured utilizing Wireshark and isolated into gadget explicit streams for disconnected examination.
    - Cleartext Identification Caught bundle streams were broken down to distinguish decoded wellbeing data. Parcels were ordered utilizing three strategies: the gullible ASCII approach, Shannon entropy, and the chi-squared test. The chi-squared test furnished the most reliable characterization with a misleading positive pace of roughly 3.5%.

Figure 4 During the data collection phase, the Withings Blood Pressure Monitor sent this image in the clear through a GET request, which reveals the nature of the device traffic

- Method Comparison: The innocent ASCII approach had a 0% bogus positive rate but missed numerous decoded bundles. The Shannon entropy technique hailed more bundles yet had a higher misleading positive rate. The chi-squared test offered a harmony among precision and bogus up-sides, distinguishing all decoded payloads with a low misleading positive rate.
- Dictionary Analysis: Cleartext parcels were looked for touchy individual data utilizing word references of normal clinical terms, individual names, and individual distinguishing data.
    - Metadata Analysis Indeed, occasional gadget use allowed inferences about client conduct even with encoded traffic. For instance, the Withings Shrewd Scale reliably spoke with a particular server, empowering the identification of its action.

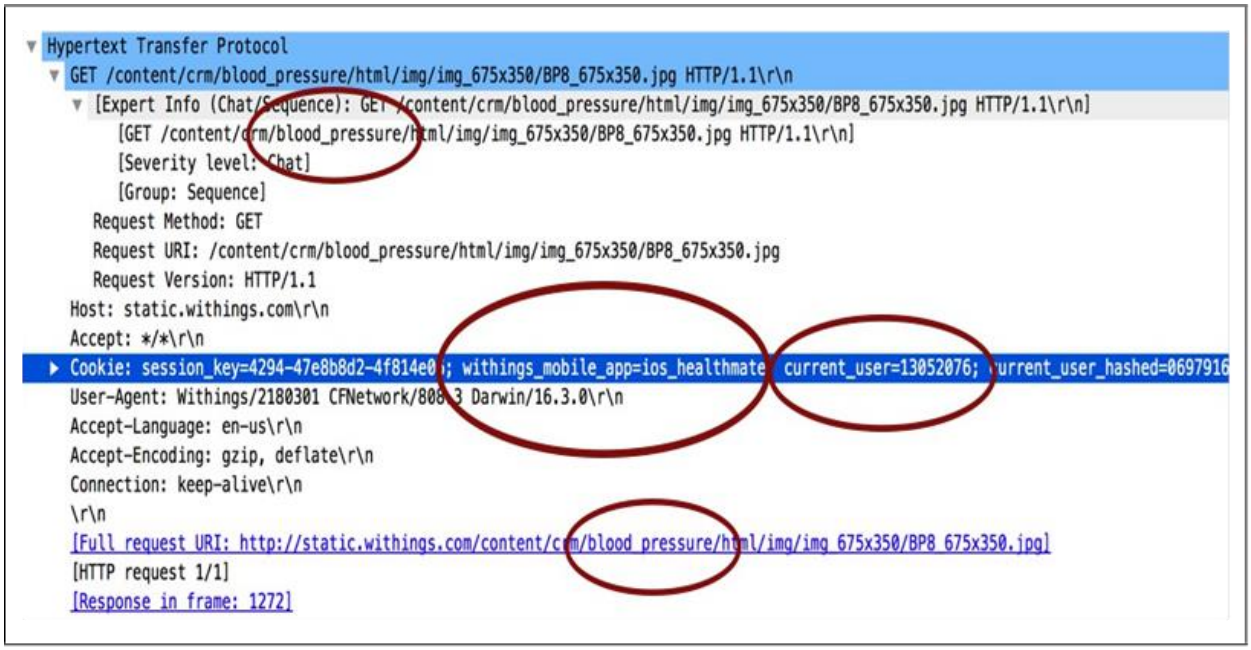

Figure 5 HTTP packet sent by IoT blood pressure monitor reveals nature of device and user behavior

4. Device weakness analysis

Significant fluctuation was observed in how clinical IoT gadgets sent information. While all gadgets utilized encryption conventions like TLS or SSH for delicate information, a few released second-request data through HTTP demands, parcel headers, and IP tables. Among the gadgets tried, the 1byOne Advanced Shrewd Remote Muscle versus Fat Scale had the most dependable execution, utilizing encryption and veiling objective names, in contrast to the Withings gadgets.

4.1. Blood Strain Screen: Holes in Cleartext

The Withings Circulatory Strain Screen displayed outstanding weaknesses. Second-request information was identified revealing client conduct, for example, the recurrence of pulse estimations. A main issue was that the gadget sent GET demand for a stock photograph after every estimation, unexpectedly telling spectators that the gadget was being used. Furthermore, metadata in the parcel contained strings like "bloodpressure" and "currentuser," which could assist with following client action and distinguish individual clients over the long run.

4.2. Scales and Glucose Screen: Encryption of Client Data

Interestingly, the Withings and 1byOne brilliant scales and iHealth pulse screen utilized TLSv1.2 to scramble client infor- mation. These gadgets communicated information safely over port 443, without uncovering the idea of the gadget or client action in the rush hour gridlock. This approach features the viability of encryption and secure conventions in safeguarding patient information.

5. Limitations

While the evidence provides valuable insights into the security and privacy vulnerabilities of IoT-enabled medical devices, several constraints must be acknowledged.

First, the evaluation was restricted to a limited number of devices, which may not represent the full spectrum of vulnerabilities in the broader market [1]. Second, proprietary restrictions prevented a comprehensive review of certain encryption methods and protocols, limiting the depth of the evaluation. Additionally, the article primarily focused on cleartext data leakage and metadata exposure, which, while significant, do not encompass all potential security risks in IoT ecosystems [2].

Moreover, the tools and techniques employed, such as packet analysis methods, may introduce false positives or fail to detect certain subtle vulnerabilities [3]. Though carefully constructed, the simulation environment cannot fully replicate real-world conditions, such as diverse traffic patterns and complex attack scenarios [4]. Lastly, generalizing the results

to all IoT-enabled medical devices requires caution, as differences in design, implementation, and use cases may lead to varying levels of security.

These constraints underscore the need for further investigation to validate and extend the insights presented in this article.

6. Ethical and regulatory implications

This article's security and privacy vulnerabilities highlight significant ethical and regulatory concerns surrounding IoT-enabled medical devices. As these devices handle sensitive electronic protected health information (ePHI), manufacturers must prioritize robust security measures to protect user data [5].

From an ethical perspective, ensuring the confidentiality and integrity of patient data is paramount. Any breach compromises individual privacy and can erode trust in IoT medical technologies, potentially hindering their adoption in healthcare [6].

Regulatory bodies like the U.S. Food and Drug Administration (FDA) and international organizations must enforce stringent security and privacy standards for IoT-enabled medical devices [7]. Compliance with frameworks like the Health Insurance Portability and Accountability Act (HIPAA) is critical, but the rapidly evolving threat landscape demands continuous updates to these regulations. Manufacturers must be held accountable for ensuring transparency in data handling practices and providing clear information to users about potential risks.

This article underscores the need for a collaborative approach involving regulators, manufacturers, and healthcare providers to address these ethical and regulatory challenges, fostering a secure and trustworthy IoT-enabled healthcare ecosystem.

7. Discussion and future work

The variety of gadgets and conventions, alongside the absence of normalization, entangles the location of weaknesses and distinguishing proof of associated gadgets. This article features the hole in adherence to HIPAA Protection and Security rules by clinical IoT producers, as delicate information and metadata about clients' way of behaving and wellbeing might be accidentally uncovered. While no actually recognizable data was spilled, makers need to encode all information and safeguard metadata.

The evaluation likewise uncovers a general absence of mindfulness among clients about classifying their information. As innovation propels, clients may not completely comprehend the degree of information that can be extricated from their computerized impressions, regardless of whether first-request data is scrambled. Devices like the one introduced here can build perceivability of weaknesses, bring issues to light, and support responsibility among makers.

Future investigations ought to consistently zero in on clinical IoT gadgets, such as brilliant glucose siphons, which might introduce novel security and protection challenges. Also, recognizing compacted and encoded traffic is vital, as makers might utilize pressure to lessen bundle sizes. Future work could incorporate AI methods to separate between these traffic types, empowering more powerful examination of packet payloads.

8. Conclusion

This article zeroed in on evaluating the organization traffic of different Web of Things (IoT) gadgets, with a specific accentuation on clinical IoT gadgets, through profound bundle inspection. This process identified a few examples of delicate client information and metadata sent in cleartext, uncovering huge security chances. These observations highlight a few weaknesses intrinsic in the plan and correspondence conventions of IoT gadgets, weaknesses that have been proven and factual in past evidence. In any case, the likely outcomes of these weaknesses are undeniably more serious with regards to clinical IoT gadgets, where the spilled metadata can give point by point experiences into a patient's medical issue and conduct.

The clinical metadata being referred to incorporates data like the recurrence of estimations, kinds of readings, and examples of gadget utilization. These are all critical for keeping up with protection and shielding patient secrecy. The incidental spillage of this data raises serious worries about the sufficiency of current security assurances for patients

utilizing associated medical care gadgets. Clinical IoT gadgets represent a one-of-a-kind test as they join both individual wellbeing information and delicate standards of conduct, making them profoundly powerless to security infringement.

Given the ramifications of these weaknesses, it is fundamental that administrative bodies, for example, medical services specialists and clinical gadget controllers, work intimately with makers to address these worries. Expanded examination of clinical IoT gadgets is important to guarantee that they fulfill rigid protection guidelines before they are carried out for boundless use in medical services settings. Furthermore, medical services experts and doctor networks should know about the potential protection chances related with utilizing IoT gadgets to screen patient vitals overstretched periods.

While clinical IoT gadgets hold tremendous commitment in further developing medical services and patient checking, their security and protection should be fundamentally improved. By taking on better encryption strategies, veiling metadata, and guaranteeing thorough protection conventions, the dangers of information spillage and unapproved access can be limited. As innovation develops, the business should stay watchful and proactive to guarantee that the security of patients isn't compromised in that frame of mind of advancement.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] A. Apostu, F. Puican, G. Ularu, G. Suciu, and G. Todoran, “Security and privacy in cloud computing: A comprehensive survey,” Procedia Computer Science, vol. 3, pp. 244–250, 2013.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” Computer networks, vol. 76, pp. 146–164, 2015. https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971?via%3Dihub

[3] S. Zeadally and O. Bello, “IoT security, privacy, and reliability: Challenges and solutions,” International Journal of Network Management, vol. 26, no. 6, pp. 425–434, 2016.

[4] E. Bertino and M. A. R. Islam, “Data security and privacy in iot: Models, algorithms, and implementations,” ACM Transactions on Internet Technology (TOIT), vol. 18, no. 1, pp. 1–22, 2017

[5] FDA, “Cybersecurity for networked medical devices containing off-the-shelf (ots) software,” U.S. Food and Drug Administration Guidance Document, 2023. [Online]. Available: https://www.fda.gov/media/119933/download

[6] U. D. of Health and H. Services, “Summary of the hipaa privacy rule,” Health Information Privacy, 2013. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[7] M. Gupta and A. Shukla, “The role of cybersecurity in healthcare data protection,” Journal of Healthcare Engineering, vol. 2020, pp. 1–9, 2020.