Internet of Healthcare Things (IoHT): Towards a Digital Chain of Custody

Lalitha Donga, Rajendra K. Raj, and Sumita Mishra
Golisano College of Computing & Information Sciences
Rochester Institute of Technology
Rochester, New York, USA
Lalitha.Donga@mail.rit.edu, Rajendra.K.Raj@rit.edu, Sumita.Mishra@rit.edu

***Abstract*—Smart Internet of Healthcare Things (IoHT) have the potential to transform patient care dramatically at reduced cost. The reality, however, is that there are serious security and privacy concerns that prevent this goal from being accomplished. The vast amounts of data being generated need to be kept secure to prevent harm to patients' health and privacy. For example, a cyberattack on heart rates data could cause patients to be over- or under-prescribed, causing severe consequences, including death. In this new environment, not ensuring a proper digital chain of custody leads to digital forensics challenges that could impact a criminal or malpractice investigation.**

This project explores enhancements needed to ensure security and privacy when IoHT are to be used in healthcare. A model is proposed to ensure a secure digital chain of custody for IoHT using database auditing techniques. The current status of the proposed concept and future directions are also discussed.

***Index Terms*—Internet of Healthcare Things (IoHT), Internet of Things (IoT), Digital Chain of Custody (DCoC), Security, Privacy, Digital Forensics**

I. Introduction

Internet of Healthcare Things (IoHT), that is, the Internet of Things (IoT) used in healthcare, are becoming increasingly popular as they can help to improve patient care in several ways, including accuracy, reliability, convenience, ease of use, and continuous connectivity [1], [2]. For example, newer wearable IoHT, such as smartwatches and fitness trackers, can measure vitals about individuals, including body temperature, heart rate, oxygen saturation, sleep quality, blood pressure, glucose levels, and much more [3].

As healthcare professionals continue to incorporate these devices into improving patient care, wide-spread automated use of IoHT requires addressing their security and privacy concerns. In particular, a secure digital chain of custody is needed to conform to current laws and practices in healthcare and cybersecurity [4], [5].

This project takes a data-centric view of incorporating IoHT into a healthcare environment, as shown in Fig. 1. The patient's healthcare data (such as heart rate and oxygen saturation), as well as other related data (such as steps walked and calories burned) being monitored by the IoHT is captured and sent to the IoHT app on the patient's smartphone. Relevant health data is then extracted and sent to the patient's hospital system for storage and analysis. After the doctor receives and analyzes the health data, a notification is sent to the patient through the IoHT smartphone app and the IoHT.

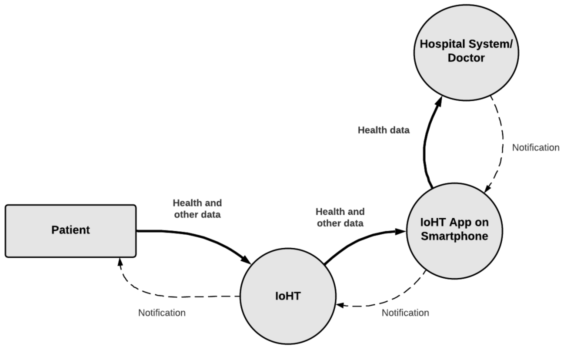

Fig. 1. A High-Level View of Using IoHT in Healthcare

We discuss one specific use case of how IoHT data can be automatically transferred to a hospital system for patient care. Abnormal readings from the IoHT could trigger data transfer and a notification to their healthcare provider, resulting in an appropriate diagnosis and prescription of any needed medication. If IoHT data security and privacy is not taken into account in this case, a cyberattack could have lethal consequences. For example, a cyberattack on an IoHT monitoring heart rates, could modify the data to show abnormally high heart rates over a long period of time, resulting in an erroneous prescription that could worsen the patient's condition. The attack could also breach sensitive health information violating the HIPAA privacy rule [6] and compromise data integrity violating the HIPAA security rule [7].

We therefore need to resolve several technical challenges when data from automated IoHT usage is used in healthcare: preventing potential harm to patient care, violating patient privacy, making healthcare data tamper-proof, and supporting digital forensics. To this end, consider a traditional chain of custody (CoC), as defined by CISA [8]:

> A process used to track the movement and control of an asset through its lifecycle by documenting each person and organization who handles an asset, the date/time it was collected or transferred, and the purpose of the transfer.

We hypothesize that proactively creating a Digital Chain of Custody (DCoC) will address many if not all of the technical challenges in the automated IoHT usage, especially system transparency and accountability. It allows us to ensure data integrity and to preemptively set up end-to-end non-repudiation and identity propagation using established standards for digital evidence management [9]. We explore steps toward setting up a secure chain of custody when IoHT are being used, and develop a proposal for an end-to-end proactive chain of custody when using IoHT.

II. Proposed Digital Chain of Custody Model

This section develops our proposed DCoC model and its usage in healthcare. Building from CISA's definition of a traditional CoC [8], we observe that a DCoC needs to deal with several situations that are not needed or possible in the traditional CoC setting. For one thing, many, if not most, investigations in this DCoC setting occur after the asset, such as the entire system or any component, has been compromised, and investigation is already underway.

When designing a DCoC, it therefore is important to be proactive in viewing the chain in its entirety to prevent a break in the chain. As CISA views it [8], a break describes a period when control of an asset is not known with certainty. Cyberattacks are frequent in the healthcare area, and consequences of violating security and privacy are severe: financial losses, legal penalties, and reputation loss [10].

Given the above consequences, it makes sense for any healthcare organization planning on future automated use of IoHT to consider the entire lifecycle:

1) Before any breach: plan out what can be done to preserve the entire chain of custody
2) During a breach: monitor and prevent any data from leaking from or getting modified
3) After a breach: use traditional database auditing techniques, as discussed below

Stoyanova et al. [9] reports that the use of IoHT requires the DCoC to be established and maintained continually to both gather and analyze the evidence or digital data. A DCoC that uses the large amounts of data from IoHTs becomes a large-scale distributed data management problem requiring the preservation of data security and privacy.

As a DCoC is a data management problem comes the solution approach: the use of traditional database auditing techniques to proactively ensure that the chain remains unbroken during the identification, preservation, and collection of data, both at the IoHT and elsewhere in the system.

Consider Fig. 1 once again, but from a data management perspective. Security of this data can be viewed as:

1) Security of *data at rest* within the IoHT
2) Security of *data in transit* between the IoHT and the corresponding smartphones
3) Security of *data at rest* within the smartphones
4) Security of *data in transit* from the smartphones to the hospital database systems
5) Security of *data at rest* in the hospital database systems

Constructing a DCoC with IoHT requires primary attention to data security in the first five of these stages. For this project, we focus on the steps involving the IoHT as protecting data in hospital systems is constantly being addressed due to compliance with the HIPAA Security Rule [7].

Solutions to preventing the occurrence of broken chains in DCoCs then becomes the use of the appropriate techniques from database auditing textbooks, such as Ben Natan [11], or commercial systems such as Oracle [12]. Auditing techniques help to track data movement through its identification, preservation, and collection phases. Other database techniques, such as Write-Ahead Logging [13] used to implement database transactions, can be adapted to work during the two data-in-transit stages in our DCoC model.

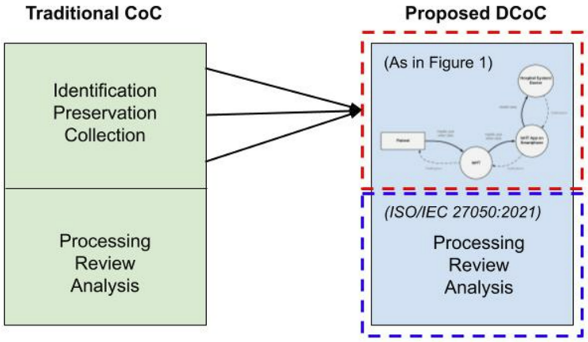

Fig. 2. Traditional vs Proposed Chain of Custody per ISO Standards

Fig. 2 shows our proposed model for a DCoC using an approach that builds on Neito et al. [4]. The six stages of a traditional CoC are shown in the left pillar of this figure while our model is shown on the right pillar. The top half of the right pillar includes our data flow diagram, shown earlier in Fig. 1, which subsumes the identification, preservation and collection phases of all the data, including the data from IoHT. The bottom half of the right pillar shows compliance with the ISO/IEC 27050:2021 standard, similar to the the standardization effort favored by Neito et al. [4]. Like their model, the elements used to build our DCoC support data integrity (tamper-proof), non-repudiation (allow IoHT data to be bound to the corresponding user's identity), delegation (allow identity propagation within the system), and standards conformance (follow established standards for digital evidence management process).

III. Current Status

By emphasizing and giving a central role to data in the digital chain of custody for IoHT, we are able to utilize traditional ideas of database security in this problem space. It allows us to use well-known techniques for distributed data auditing to move toward a framework for a DCoC for flexible inclusion of data from IoHT.

This project introduces this novel DCoC concept based on database auditing and attribute-based access control. We plan to prototype parts of this framework using IoHT, validate its ability to be a true DCoC (including support for digital forensics), and perform preliminary benchmarks.

Acknowledgments

Donga and Raj acknowledge support by the National Science Foundation under Award 1922169.

References

[1] Omaha Media Group, "Why IoT is Becoming Increasingly Popular in Consumer Products," Mar. 2018. https://www.omahamediagroup.com/blog/article/why-iot-is-becoming-increasingly-popular-in-consumer-products.

[2] Chiron Health, "What is Telemedicine?," 2022. https://chironhealth.com/telemedicine/what-is-telemedicine/.

[3] Behr Tech, "Top 10 IoT Sensor Types," 2020. https://behrtech.com/blog/top-10-iot-sensor-types/.

[4] A. Nieto, R. Rios, and J. Lopez, "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 642–649, 2017.

[5] S. Watson and A. Dehghantanha, "Digital Forensics: the Missing Piece of the Internet of Things Promise," *Computer Fraud & Security*, vol. 2016, pp. 5–8, 2016. http://usir.salford.ac.uk/id/eprint/39539/.

[6] US Department of Health & Human Services, "HIPAA Privacy Rule," 2021. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[7] US Department of Health & Human Services, "HIPAA Security Rule," 2013. https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[8] US Cybersecurity and Infrastructure Security Agency, "CISA Insights: Chain of Custody and Critical Infrastructure Systems," 2021. https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf.

[9] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[10] S. Alnefaie, A. Cherif, and S. Alshehri, "Towards a Distributed Access Control Model for IoT in Healthcare," in *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, pp. 1–6, 2019.

[11] R. Ben Natan, *Implementing Database Security and Auditing*. Burlington, MA: Digital Press, 2005.

[12] Oracle Corporation, "Database Auditing: Security Considerations," 2022. https://docs.oracle.com/cd/B19306_01/network.102/b14266/auditing.htm#CHDJBDHJ.

[13] C. Mohan, D. Haderle, B. Lindsay, H. Pirahesh, and P. Schwarz, "ARIES: A Transaction Recovery Method Supporting Fine-granularity Locking and Partial Rollbacks using Write-ahead Logging," *ACM Transactions on Database Systems (TODS)*, vol. 17, no. 1, pp. 94–162, 1992.