A Proactive Digital Chain of Custody for Internet of Healthcare Things (IoHT) Data

Lalitha Donga, Shreya Pramod, Sumita Mishra, and Rajendra K. Raj
Golisano College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, NY 14623, USA
[lalitha.donga, sp3045, sumita.mishra, rajendra.k.raj]@mail.rit.edu

***Abstract*—The increased use of the Internet of Healthcare Things (IoHT), i.e., Internet of Things devices used in healthcare, highlights the need to support continuous gathering and maintenance, leading to challenges in preserving healthcare data security and privacy. This paper briefly examines these challenges and proposes an end-to-end proactive Digital Chain of Custody (DCoC) when using IoHT. It outlines an IoHT-DCoC using concepts, such as data accountability using datakeeper software and dynamic data logging built on data encryption. Finally, an attribute-based access control (ABAC) model is developed that proactively ensures end-to-end data security and privacy.**

***Index Terms*—Internet of Things, Internet of Healthcare Things, Digital Forensics, Digital Chain of Custody, Data Security and Privacy, Data Integrity, Health Data Regulations**

I. Introduction

The Internet of Healthcare Things (IoHT), i.e., the Internet of Things (IoT) used in healthcare, have become commonplace due to their decreased costs and user acceptance, as well as their potential to improve patient care in terms of accuracy, reliability, convenience, ease of use, and continuous connectivity [1]. Wearable IoHT, such as smartwatches or specialized devices, can measure many vitals, including body temperature, heart rate, oxygen saturation, sleep quality, blood pressure, and glucose levels [2]. The widespread use of IoHT requires *following the data* to ensure its security and privacy and compliance with established practices in healthcare [3].

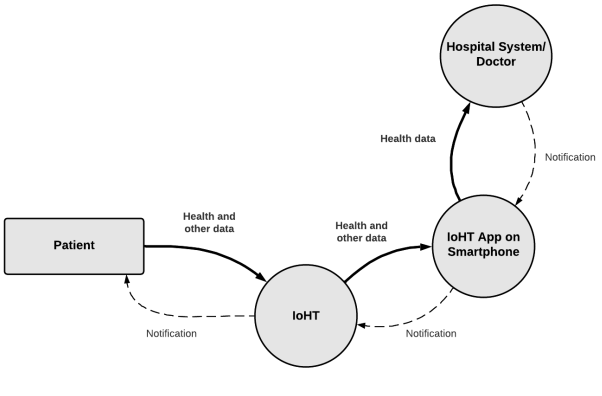

Fig. 1. A High-Level View of Using IoHT in Healthcare [4]

Fig. 1 [4] emphasizes a data-centric view in incorporating IoHT into a healthcare environment. Electronic Protected Healthcare Information (ePHI), such as heart rate, oxygen saturation or steps walked, generated by IoHT are typically delivered to the patient's smartphone first and then perhaps sent to the patient's hospital system for storage and analysis. After analysis by a medical professional, a response notification is sent to the patient through their IoHT smartphone app, even perhaps to the IoHT device [5].

Cyberattacks on ePHI in 2023 affected over 540 organizations and 112 million individuals, more than doubling the impact on individuals from the previous year [6]. Such attacks could have lethal consequences unless IoHT data security and privacy needs are addressed. For instance, a cyberattack on an IoHT monitoring heart rates could change the data to show abnormally high heart rates over a long period, resulting in an incorrect diagnosis and prescription that could worsen the patient's condition. The attack could also breach sensitive ePHI in violation of the US HIPAA Privacy Rule [7] while ePHI modification would violate the HIPAA Security Rule [8]. The resulting ePHI modifications would worsen future digital forensic analyses [9].

The legal concept of *Chain of Custody* refers to the custody, control, transfer, analysis, and disposition of evidence, both physical and electronic. It is defined by the US Cybersecurity and Infrastructure Agency (CISA) as [10]:

> *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.*

A *Digital Chain of Custody (DCoC)* thus represents the route that digital data takes from the start to the end of its life cycle and ensures the sanctity and safety of the data. Developing an IoHT-DCoC addresses several technical challenges and helps with system transparency and accountability [11].

It also preemptively ensures data integrity and sets up an end-to-end non-repudiation and identity propagation using established standards for digital evidence management. Stoyanova et al. [9] highlight the need for continuous maintenance and gathering of data in an IoHT-DCoC. As the usage of healthcare data increases many-fold when IoHT are used, the need to protect data continuously becomes more crucial. Key requirements for IoHT data include:

- **Building Patient Trust:** Patients are more likely to trust healthcare providers when they have confidence that their data is safeguarded.
- **Meeting Regulatory Requirements:** Healthcare data is subject to local regulations, such as the US HIPAA law.
- **Ensuring Data Integrity:** Maintaining the integrity of records and preventing access or tampering is crucial for accurate diagnosis and treatment.

This paper investigates the creation of an IoHT-DCoC. It has two contributions: (a) a high-level design of an end-to-end proactive IoHT-DCoC, and (b) an attribute-based access control (ABAC) model to support end-to-end proactive requirements for data security and privacy.

Section II examines the relevant related work. Section III outlines the end-to-end proactive DCoC for using IoHT, while Section III discusses our proof-of-concept implementation. Section V develops an attribute-based access control (ABAC) model for maintaining our end-to-end proactive DCoC. We conclude with a few final remarks about the status of this work and future directions.

II. Related Work

Almost a decade ago, Intel claimed that "half of all care will be delivered virtually, with providers paid based on their teamwork and quality." [12]. Although this claim has not materialized yet, the COVID-19 pandemic accelerated remote care adoption: "telehealth use has increased 38X from the pre-COVID-19 baseline" [13], with needed work being carried out in practitioner circles in IoHT [14]. The quality and capability of IoHT devices are critical as IoHT must remain reliable even during data overloads [15]. With expanded features (e.g., fall detection, EKG monitors, sleep apnea, glucose monitoring, and UVA and UVB exposure detection), greater reliability, and lower prices, the use of IoHT will increase, resulting in a greater need for DCoCs.

Practitioners and academic researchers have attempted to address security and privacy concerns in healthcare. Watson and Dehghantanha [16] examine challenges to digital forensics for IoHT. For DCoC designs and approaches, Neito et al. [3] proposed the notion of a "digital witness", which is tamper-proof, allowing IoHT to be tied to a user's identity and for this identity to be delegated and propagated throughout the system for non-repudiation. Rather than tying the IoHT to a user's identity, our solution instead ties a data keeper to each sensor in the IoHT, as well as linking access control to each point in the IoHT lifecycle (data in transit to and from the IoHT, smartphone app, and hospital system). Other efforts to create DCoCs include mechanisms such as blockchains [11], [17]. As discussed later, to lower costs, our solution avoids blockchains.

As an advanced ledger, Dynamic Source Trace (DST) enables real-time tracking of patient health records [18] using blockchains. Using immutable logs for all ePHI access and modification, DST is claimed to provide greater transparency, traceability, and efficiency compared to conventional database logging. DST also supports machine learning algorithms to enable real-time detection and alerting of unauthorized data access or modification of ePHI [19], as well as scalability.

Traditional database auditing can track and proactively fix broken chains in DCoCs [20]. Auditing techniques help track data movement through identification, preservation, and collection phases. Our solution uses logging techniques, making it similar to database auditing.

Tomas and Jordi [21] focus on medical image authentication using an Image Signature Matrix (ISM) that combines biometric-based encryption mechanisms with unique image signatures to identify and flag corrupted or fake images efficiently. Authentication is not our focus here but future work can use such authentication methods in an IoHT-DCoC.

Yuan et al. [22] emphasize machine learning (ML) algorithms to detect unauthorized access to the data, as manual intervention at every point becomes tedious and technically infeasible with the increasing amount of healthcare data. The ML model learns from existing legitimate access patterns and raises alerts upon detecting anomalies to deal with unauthorized access promptly. These patterns help support a proactive IoHT-DCoC. Our proposed solution, however, focuses on access control and logging to support a proactive IoHT-DCoC.

Any IoHT-DCoC must be aware of legal considerations, for instance, different countries have laws governing the use of IoHT. For example, the US Federal Drug Administration (FDA) governs the approval of all medical devices sold in the US [23]. California also has been at the forefront of regulating the IoHT market, requiring devices connecting to the internet must have "reasonable security features" that prevent unauthorized access, modification, or data exposure [24].

Our overall focus in this paper is somewhat different from most of the above-related work, as we focus on building a proactive IoHT-DCoC that supports continuous gathering and maintenance of IoHT data to ensure ePHI security and privacy.

III. The Proposed Digital Chain of Custody Model

This section discusses our proposed DCoC model for IoHT data. As stated, we rely on a data-centric approach and access control mechanisms for our proposed DCoC model.

A. Background

To build from CISA's definition of a traditional CoC [10], we first observe that DCoCs have several new challenges that do not exist in conventional CoC settings. For example, it is common for traditional DCoC investigations to begin only after the entire system has already been compromised.

A break in the chain of custody is the period when control of an asset is not known with certainty [10]. To prevent such breaks, we categorize the entire lifecycle in terms of any breach: *before*, *during*, and *after*. We achieve this by combining preventive, monitoring, and logging techniques. All of these are required in healthcare as cyberattacks may occur frequently and unexpectedly. Not only is ePHI subject to legal requirements and ethical considerations, but it is also life-critical, as even a minor cyberattack on a healthcare system could result in dire consequences for patients in terms of death, and for healthcare providers in terms of financial or reputation loss, not to mention legal penalties [25]. As a result, an IoHT-DCoC needs to ensure continuous maintenance and gathering of digital data [9]. Managing the breadth, depth, and quantity of healthcare data in an IoHT-DCoC is akin to a large-scale distributed data management problem, helping the prevention of a break in the chain [9]. Creating an IoHT-DCoC requires attention to both data at rest and in transit. Securing data within the IoHT complies with the HIPAA Security Rule [8].

B. Model Features

Our proposed DCoC model for IoHT has the following features:

- **Data Logging:** All interactions with the data are logged in real-time: data creation, data modification, up to data deletion. As a result, the process is transparent and easily traceable if there are data breaches.
- **Time-stamping:** All IoHT data interaction gets time-stamped to provide the correct order of the data events. This assists not only in establishing a proper sequence of data flow but also in identifying unauthorized access.
- **Datakeeper software:** Assigning datakeepers at every point of the data life cycle ensures data accountability. Each *datakeeper* is responsible for ensuring the safety of the data and checking whether all the protocols are strictly followed.
- **Encryption & Digital Signatures:** Proper approaches to encryption are needed throughout the processes of DCoC to ensure that the data being transferred digitally stays confidential and tamper-proof.

The IoHT-DCoC framework is strengthened using ABAC as discussed in Section V to support the working of datakeeping. We thus rely on attributes associated with data: subjects (datakeepers or associated individuals), objects (actual healthcare records), and environment(s) (in which access is utilized).

IV. Methodology

As stated earlier, the integrity of IoHT data must be maintained throughout its lifecycle. We focus on ensuring systematic capture and identification of each datakeeper transition to increase data security and transparency.

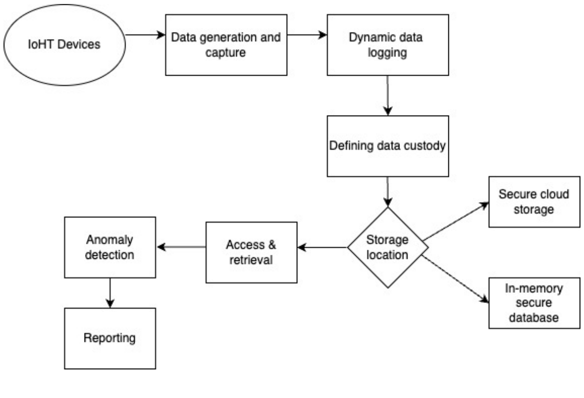

Fig. 2. IoHT Data Lifecycle

TABLE I
Sample Data

idx	data source	timestamp	values
0	spo2	13:37:38.0	[99]
1	spo2	13:37:38.0	[89]
2	ambient_light_sensor	13:37:38.0	[1087]
3	accelerometer	13:37:38.0	[-5.220675, 8.682511, 13.000555]
4	heart_rate	13:37:38.0	[61]
5	battery	13:37:38.0	[100]
6	magnetometer	13:37:38.0	[-12.319649, 87.12794, -71.551858]
7	gyroscope	13:37:38.0	[-3.009747, -3.159155, -3.096995]
8	ambient_light_sensor	13:37:38.0	[6373]
9	orientation	13:37:38.0	[-4.270139, -48.179149, 58.15792]
10	accelerometer	13:37:38.0	[-1.559278, 0.638313, 12.642135]
11	battery	13:37:38.0	[90]
12	barometer	13:37:38.0	[30.087588074195057]
13	magnetometer	13:37:38.0	[41.767118, -83.394388, 77.071183]
14	ambient_light_sensor	13:37:38.0	[1270]

TABLE II
Data Custody

Sensor Type	Keeper
spo2	Keeper A
accelerometer	Keeper B
heart_rate	Keeper C
magnetometer	Keeper D
gyroscope	Keeper E
orientation	Keeper F
ambient_light_sensor	Keeper G
barometer	Keeper H
temperature	Keeper I
battery	Keeper J

Fig. 2 shows the IoHT data lifecycle. It describes a flow sequence beginning with the IoHT devices that extract health-related data. The process then dynamically logs this extracted data, which is then assigned to the respective datakeeper software to maintain data integrity and privacy. This is then stored in designated digital storage, e.g., secure cloud databases, which supports remote accessibility, further assisted by in-memory data reserves to allow faster data retrieval. This approach helps with anomaly detection for quicker identification of health concerns. The data cycle ends with the reporting phase that assists healthcare providers in making clinical decisions. This approach highlights the criticality of secure and precise data handling in healthcare data management.

Table I demonstrates datakeeping using sample data from a table comprising 200,472 records, which were simulated from similar data shown in various sources, especially from Healthcare.gov [26]. Sources were selected based on common sensors used in smartwatches, such as accelerometers, barometers, gyroscopes, heart rate sensors, and more [27].

We have attempted to ensure the overall data is comprehensive to permit sufficient analysis of typical data interactions to serve as a proof-of-concept of our proposed DCoC. The sample dataset was obtained by running a Python script to simulate the performance of IoHT devices. Random values were generated to populate this dataset. A much larger study based on real healthcare data would be needed to validate our ideas.

The methodology guiding our proof-of-concept follows.

- **Defining Datakeeping:** Identifying and analyzing the data journey is the pivotal part of our approach. The initial goal is to understand and accumulate all the data interaction points of contact, which includes IoHT. At each contact point, based on the sensor type that the data is generated from, a unique datakeeper is assigned. Each datakeeper also tracks the next datakeeper to which the data is sent, avoiding data leakage or corruption and allowing anomalies to be traced back to their origin [4]. Per Table II, datakeeping is defined with the sample data, which establishes the various data interaction points extracted from the IoHT, such as SpO2, accelerometer, and heart rate [27]. The data contains 10 unique points of interaction that are categorized as follows: Device Sensor Data (e.g., SpO2 or heart rate), Ambient Sensor Data (e.g., ambient light sensor or temperature), and Device System Info (e.g., battery).

A unique datakeeper is assigned to each data interaction point. Thus, if any data leakage occurs, for instance on the gyroscope, then Keeper E would have the required information to gain more details on the data leak. For patient data breaches, datakeeper software assigned at each point of contact would be analyzed to trace the breach's origin. Proper tracking of datakeeper software enables pointing to the exact source of the data breach.

- **Dynamic Data Logging:** During each data transition from the points of contact, it is necessary to log the data to ensure a continuous chain of custody as depicted in the code snippet indicated in Table II. Each of the data interactions would be time-stamped to enable easier data access. The data columns must include the index, source, timestamp, encrypted values, category, and the assigned keepers. We have used the pandas DataFrame [28] to log interactions at every point.
- **Data Encryption:** To supplement data integrity supports, we use encryption by linking each data element with a unique digital signature to help with data validation. For each transition, it is essential to have an end-to-end encryption system in place.

```
log_df = pd.DataFrame(columns=log_columns)

for idx, row in df.iterrows():
  log_entry = pd.DataFrame({
    ’index’: [row[’index’]],
    ’source’: [row[’source’]],
    ’timestamp’: [row[’timestamp’]],
    ’values’: [encrypt_data(cipher,
      str(row[’values’]))],
    ’Category’: [row[’Category’]],
    ’Assigned Custodian’:
      [row[’Assigned Custodian’]]
})
log_df = pd.concat([log_df, log_entry],
  ignore_index=True)
log_df[’values’] = log_df[’values’].apply(
  lambda x: decrypt_data(cipher, x))
log_df.to_csv(
  ’data_interaction_log.csv’, index=False)

print(”Data interactions logged and encrypted!”)
```

Fig. 3. Data Logging

A. Challenges and Future Directions

Although implementing DCoC in real-world scenarios within complex healthcare systems presents challenges it is still called for, as discussed earlier. The dynamic nature of data storage, rapid technological advancements, and evolving threats require adaptable DCoC frameworks. Leveraging technologies, such as blockchain and machine learning, may also offer security and transparent handling of electronic health data.

V. Attribute-Based Access Control Model

Proper access control is needed to keep patient data secure in the proposed IoHT-DCoC. Access control is defined in the first Technical Safeguard Standard of HIPAA's Security Role as "the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource" [8]. Even if a user is generally authorized, the amount of information they can access must still be controlled using appropriate policies. For instance, to prevent improper use of data and protect patient privacy, only the primary care physician needs access to a patient's data. As such, we adopted a performant variant of attribute-based access control called BLAC for our IoHT-DCOC [29].

To help maintain the end-to-end digital chain of custody and improve the security of IoHT, we designed a data flow model using attribute-based access control (ABAC) [30]. ABAC typically uses a complex set of *rules*, rather than *roles*, to define who gets access privileges to a system. Attributes about a person are used to authorize an individual. Consider a doctor. On initial setup, their credentials, such as degree certificates, board certifications, and licenses, are used to establish that they have the *attributes* of a doctor. When they authenticate into a system, their system-stored credentials would constitute an attribute to establishe that they are a doctor. ABAC is more secure than Role-Based Access Control (RBAC), which relies only on the *artificial* role that a system administrator has assigned them. This could be problematic from a data security and privacy point of view because a *Doctor* role could be assigned inadvertently or maliciously to a *Pharmacist* and the system would not know any better! ABAC ensures confidentiality in IoHT because only correctly credentialed users can access the data.

Although IoHT health data may not form a traditional medical report, it still must be protected. Our access model focuses on how ABAC needs to be enforced when IoHT are used to send health data to a provider.

The overall data flow model with ABAC is shown in Fig. 4. This data flow model is adapted from Alshehri et al. [29] for IoHT data. The integrated data flow model discussed here incorporates an access control decision engine in the end-to-end data flow process shown earlier in Fig. 1.

A. Components of the Access Model

Systems: The main elements that exchange health data in our access model are the IoHT, the IoHT smartphone, and the hospital system. The health data collected by the IoHT is

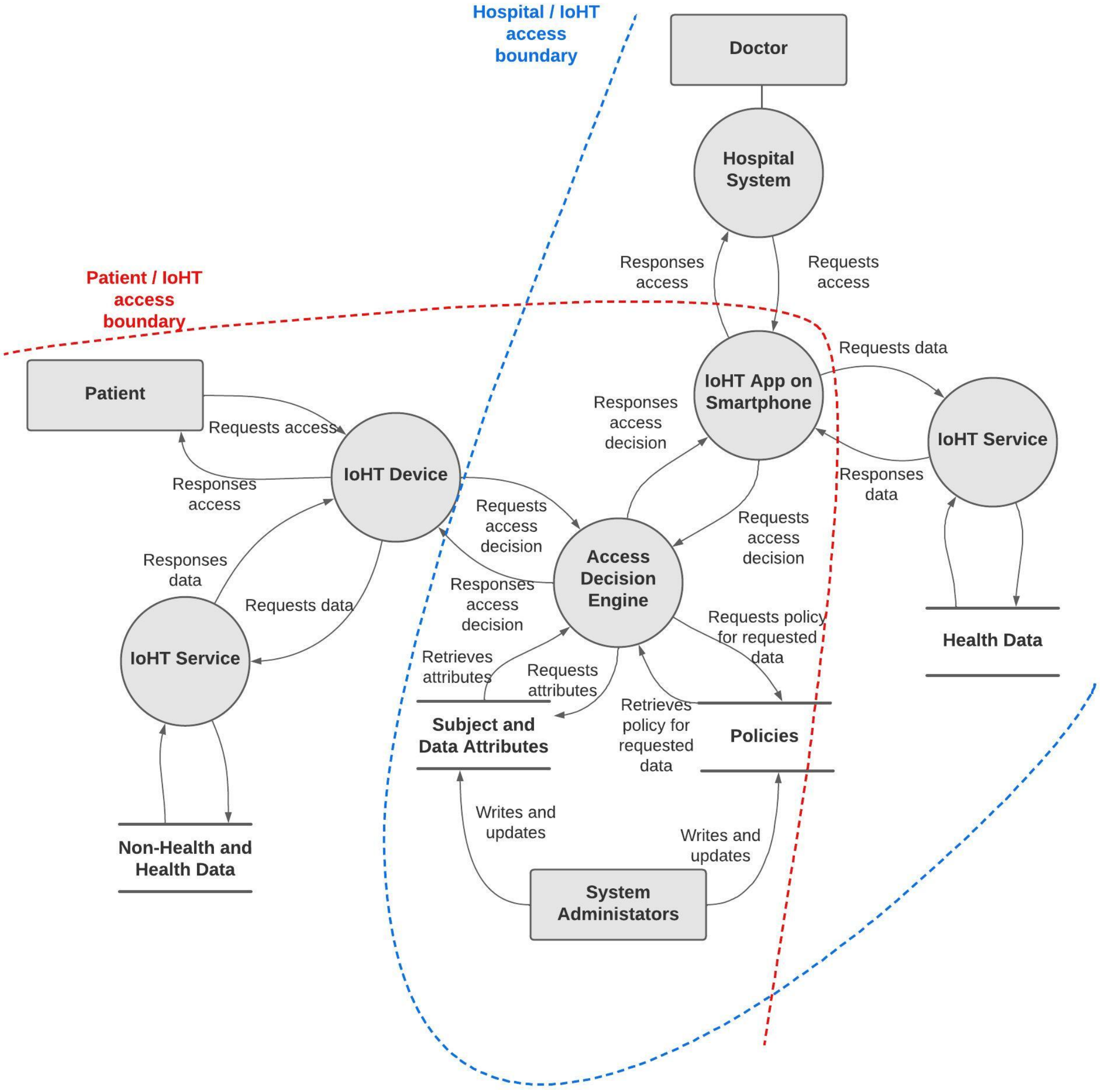

Fig. 4. Access Control Model for IoHT

transferred to the hospital system, via the IoHT smartphone app, for further analysis by authorized medical professionals.

Users: The main users interacting with these systems are the patients, the system administrators, and the authorized medical professionals, such as physicians, nurses, administrative, and billing staff. Each *patient* is a user who gets their health data tracked by the IoHT and delivered to an authorized hospital system while *authorized medical professionals* receive health data from the patient. The patient could be the system administrator for some system elements, e.g., the IoHT, while the hospital personnel could manage other elements, e.g., hospital databases.

The approach relies on attributes associated with data: subjects (the datakeepers or the associated individuals), objects (the actual healthcare records), and the environment(s) in which access is needed. That is, instead of assigning a datakeeper role (as in RBAC) solely based on the user role [31], the BLAC model uses relevant attributes of the user to determine whether access is justified to each element of the data.

Access Decision Engine: The main stages in the end-to-end data transfer from the IoHT to the hospital system that require an access decision (made by the Access Decision Engine) for maintaining the IoHT-DCoC are (1) IoHT to IoHT smartphone app and (2) IoHT smartphone app to the hospital system

Services: Once an access decision is made, an IoHT service entity will respond with the corresponding requested data or deny access. This service is provided for data transfer between IoHT and the smartphone app, and between the IoHT smartphone app and the hospital system.

B. Using the Access Model

We now show how patient health data is protected from unauthorized access at the two stages: IoHT to IoHT smartphone app, and IoHT smartphone app to the hospital system. The Access Decision Engine works as follows:

1) Access Decision Engine receives a request for access
2) Access Decision Engine requests to see the policies for the requested data, set by the system administrator
3) Policies are received by the Access Decision Engine
4) Access Decision Engine verifies the request against the policies using the proposed model from Section III
5) Access Decision Engine requests to see the subject and data attributes for the requested data, set by the system administrator
6) Subject and data attributes are received by Access Decision Engine
7) Access Decision Engine verifies the request against subject and data attributes using our proposed model
8) If the access request satisfies the received policies and subject and data attributes, Access Decision Engine will accept the request, otherwise deny it

In the hospital system, medical professionals will have attributes associated with them, such as their name, identification number (ID), field, and department. The ABAC model ensures that only authorized medical professionals of the hospital can view the patients' information.

The ABAC model discussed above thus helps to cement support for the security and privacy ePHI in our IoHT-DCoC.

VI. Final Remarks

The central role of data in the proposed IoHT-DCoC leverages traditional data security and privacy concepts, especially by the use of ABAC in this domain. We can also use established techniques for auditing, especially in distributed database settings, to move toward a flexible IoHT-DCoC.

This paper introduced a novel IoHT-DCoC based on datakeeper software, data logging, and attribute-based access control. We have tested parts of the framework to validate the feasibility of our approach and will build a full-fledged IoHT-DCoC and perform benchmarks.

Acknowledgments

We acknowledge partial support by the National Science Foundation under Awards 1922169 and 2110771.

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

[3] 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.

[4] L. Donga, R. K. Raj, and S. Mishra, "Internet of healthcare things (ioht): Towards a digital chain of custody," in *2022 IEEE 10th International Conference on Healthcare Informatics (ICHI)*, pp. 524–526, IEEE, 2022.

[5] S. S. Chopade, H. P. Gupta, and T. Dutta, *Survey on Sensors and Smart Devices for IoT Enabled Intelligent Healthcare System*, pp. 1–39. Springer Nature, 6 2023.

[6] J. McKeon, "This year's largest healthcare data breaches," Dec. 2023.

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

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

[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] 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.

[11] F. Alruwaili, "Custodyblock: A distributed chain of custody evidence framework," *Information*, vol. 12, 02 2021.

[12] Intel Corporation, "The Internet of Things and Healthcare Policy Principles," Jan. 2015. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/iot-healthcare-policy-principles-paper.pdf.

[13] McKinsey & Company, "Telehealth: A quarter-trillion-dollar post-COVID-19 reality?," July 2021. https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality.

[14] O. Manta, N. Vasileiou, O. Giannakopoulou, K. Bromis, I. Kouris, M. Haritou, G. Matsopoulos, and D. Koutsouris, *Enhancing Healthcare Through Telehealth Ecosystems: Impacts and Prospects*, vol. 309, pp. 302–303. IOS Press Ebooks, 10 2023.

[15] M. Martynenko, "Internet of things in healthcare: What you should know to make it right," Mar. 2021. https://www.aimprosoft.com/blog/iot-in-healthcare-benefits-challenges-cases/.

[16] 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/.

[17] M. Chopade, S. Khan, U. Shaikh, and R. Pawar, "Digital forensics: Maintaining chain of custody using blockchain," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 744–747, 2019.

[18] K. C. Bandhu, R. Litoriya, P. Lowanshi, M. Jindal, L. Chouhan, and S. Jain, "Making drug supply chain secure traceable and efficient: a blockchain and smart contract based implementation," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 23541–23568, 2023.

[19] K. Shuaib, H. Saleous, K. Shuaib, and N. Zaki, "Blockchains for secure digitized medicine," *Journal of personalized medicine*, vol. 9, no. 3, p. 35, 2019.

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

[21] T. Marques-Arpa and J. Serra-Ruiz, "Prs signal in acquiring evidence of digital chain of custody," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 273–278, IEEE, 2016.

[22] B. Yuan, Y. Jia, L. Xing, D. Zhao, X. Wang, and Y. Zhang, "Shattered chain of trust: Understanding security risks in Cross-Cloud IoT access delegation," in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 1183–1200, USENIX Association, Aug. 2020.

[23] US Food & Drug Administration, "Medical Devices," 2022. https://www.fda.gov/medical-devices.

[24] State of California, "Sb-327 information privacy: connected devices," Jan. 2020. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[25] 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.

[26] U.S. Centers for Medicare & Medicaid Services, "Healthcare Datasets," 2024. https://data.healthcare.gov/datasets/.

[27] Fitbit, "Fitbit API: Sensor Guides." https://dev.fitbit.com/build/guides/sensors/.

[28] Pandas Development Team, "pandas-dev/pandas: Pandas," Feb. 2020.

[29] S. Alshehri, S. Mishra, and R. K. Raj, "Using access control to mitigate insider threats to healthcare systems," in *2016 IEEE International Conference on Healthcare Informatics (ICHI)*, pp. 55–60, 2016.

[30] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[31] S. Alshehri and R. K. Raj, "Secure access control for health information sharing systems," in *2013 IEEE international conference on healthcare informatics*, pp. 277–286, IEEE, 2013.