

Article

Decision Model to Design Trust-Focused and Blockchain-Based Health Data Management Applications

Christina Erler ^{1,*} , Ann-Marit Bauer ¹, Friedrich Gauger ¹ and Wilhelm Stork ²

¹ Embedded Systems and Sensors Engineering, FZI Research Center for Information Technology, DE-76131 Karlsruhe, Germany; bauer@fzi.de (A.-M.B.); gauger@fzi.de (F.G.)

² Institute for Information Processing Technologies, Karlsruhe Institute of Technology, DE-76131 Karlsruhe, Germany; wilhelm.stork@kit.edu

* Correspondence: erler@fzi.de

Abstract: Many Blockchain-based approaches have been published in the field of health data management applications (HDMAs). However, no comprehensive guideline exists to guide the multiple and interdependent design decisions to develop such systems. This paper aims to support the HDMA system design processes by introducing a novel decision model. The model considers all relevant requirements, from regulatory context to user needs and trust considerations. To generate the decision model, we define a taxonomy that organizes previously published approaches by their technical design features and combines it with the trust assumptions of the participating actors according to the STRIDE method. The model aims to support a cohesive overall system design by addressing Blockchain type, off-chain storage, identity and access management, security decisions, and the specific use case of data donation. A group of experts evaluated the decision tree and its utility is demonstrated in three representative use cases. Special attention is paid to the use case of data donation via a data trustee, which is examined in detail.

Keywords: blockchain; distributed ledger technology; health data management; decision model; design decision; data management; medical data storage; access management; identity management; data trustee



Citation: Erler, C.; Bauer, A.-M.; Gauger, F.; Stork, W. Decision Model to Design Trust-Focused and Blockchain-Based Health Data Management Applications.

Blockchains **2024**, *2*, 79–106. <https://doi.org/10.3390/blockchains2020005>

Academic Editors: Keke Gai and Liehuang Zhu

Received: 31 December 2023

Revised: 5 April 2024

Accepted: 6 April 2024

Published: 9 April 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction and Basics

The technological advancement in managing health data has emerged as a crucial aspect in the digital transformation of the healthcare sector [1]. Although several European countries, including Germany, have had government-regulated Electronic Health Record (EHR) systems on their political agenda for years, implementing EHR systems in most countries is behind schedule [2]. As a result, today, EHRs often exist as isolated systems maintained by specific healthcare providers with no connection between them [3]. Health data management applications (HDMA) refer to a broader understanding of computerized systems designed to gather, store, and utilize individual health status data. The potential benefits of a well-designed HDMA system, which allows for comprehensive processing, sharing, and use of medical health data, have become evident in recent years: cooperation between different care providers treating the same patient can be facilitated, thus leading to better treatment and patient outcomes. Also, HDMAs allow for higher overall efficiency of the healthcare system [4]. In addition, the donation of data collected in such a system would be useful for accelerating medical research, developing novel therapeutic approaches, and for digital health applications [5]. Data trustees are currently being discussed as a potential solution to overcome isolated HDMAs. These act as a legally compliant and neutral intermediary between a data provider and a data user [6]. Separate from government-funded initiatives, private-sector companies have pursued the objective of establishing centralized HDMA solutions, leading to the creation of data monopolies [7]. The will to share health record data with private sector companies is generally lower in the general public than it

is for sharing with public research institutions [5]. Distributed Ledger Technology (DLT) is currently being explored as a reliable and interoperable infrastructure that can preserve patients' self-determination while enabling data sharing across the public and private sectors. DLT aims to facilitate and enhance the exchange of highly sensitive patient data across different organizations in the healthcare sector while preserving trust, privacy, and security (see Section 3). The most recognized form of DLT is Blockchain, which utilizes linked lists to chain transaction histories (blocks) and creates an immutable ledger (chain) [8]. By leveraging Blockchain technology, there is no reliance on a central intermediary for trust. Instead, trust is placed in the underlying technology and its cryptographic procedures, which are designed to be tamper-resistant, transparent, and fail-safe [3,9]. These properties are the basis for a data trustee to act as a neutral authority between all health actors required to set up the HDMA.

Research and industry have actively explored and developed diverse Blockchain-based approaches to address the challenges mentioned above [10]. Within these strategies, different design patterns related to Blockchain implementations are utilized [3]. The conception of such systems encompasses many critical design decisions, which have been analyzed and structured into decision models by both Xu et al. [11] and Erler et al. [10]. The latter set out to structure these approaches and develop a guide to making appropriate technical design decisions. In order to aid design decisions of future Blockchain-based projects, Erler et al. have developed a decision model, guiding project decisions regarding the type of Blockchain to use; storage location and off-chain storage type of patient data; and encryption methods and basic security measures, such as encryption, access control, and de-identification [10]. The model allows developers to navigate design decisions based on their specific application and contextual factors. According to the authors, one weakness of the decision model is the lack of consideration of Identity Management (IdM), which goes hand in hand with suitable Access Management [10]. Xu et al. [11] have published work that presents decision models based on reviewed patterns in the design of Blockchain-based applications. They present several decision models concerned with on-chain and off-chain data storage, authentication, authorization, smart contracts, and the system's connection to the outside world. Xu et al. [11] present decision factors emphasizing the practical and technical needs of the system developer and offer arguments for each decision that describe the technical consequences of its use. According to Erler et al. (2023) [12], a systematic security requirement analysis is mandatory in the design of HDMA, accounting for the requirements and trust relationships of the system entities involved and the developers' needs. This insight motivates our research question: How can we build a comprehensive decision model based on design decisions in the conception and implementation of a Blockchain-based HDMA while considering the security and trust assumption of the involved system entities? To answer the research question, this paper adopts the applied methodology and past work of Erler et al. (2022) [10] in creating a taxonomy and a subsequent decision model. It aims to address the topics of identity and access management, which Erler et al. (2022) indicated as missing [10]. In addition, this paper tries to focus on design decision factors that address not only the needs of system developers but also consider the trust relationships between system entities to ensure the integrity of a system that relies on the trust of its participants. We deem this consideration essential for the success of such systems. In order to structure the trust analysis, the STRIDE method is applied [13], taking the lead from the example of Erler et al. (2023) [12]. Additionally, the decision model aims to generalize the use cases to which the decision model can be applied by including data trustee decision factors.

The paper is organized as follows: First, the methodology applied is explained and followed by a description of the taxonomy, which summarizes the state of the art. Next, the decision model is presented. This model is then evaluated and applied to past research use cases that have already been published. Beyond that, the decision model is used to create a design concept for a data trustee, which allows the sharing of patient data with

healthcare providers and the research community. The paper concludes with a discussion of the results and future work.

2. Methods

The design science research methodology (DSRM) of Peffers et al. [14] used by Erler et al. (2022) [10] for developing a decision model serves as the overall blueprint for the model developed herein. The DSRM includes the following six steps: (1) problem identification and motivation; (2) definition of objectives of solution; (3) design and development of the solution artifact; (4) demonstration of the solution artifact; (5) evaluation of the effectiveness and efficiency; (6) communication. In accordance with the approach of Erler et al. (2022) [10], our research began with a literature review of existing Blockchain-based approaches after the problem identification and motivation, found here in Section 1. The presented approaches were used to classify design decisions into a comprehensive taxonomy following the method by Nickerson et al. [15]. This taxonomy guided the formation of the ultimate decision model and, thus, the design and development of the solution artifact of this work. See Section 4 for a demonstration of the solution artifact and Section 5 for its evaluation. In conclusion, this paper acts as the communication step of the DSRM. In our work, the decision factors and arguments of the decision model are developed with the STRIDE-based trust barriers in mind [13]. Erler et al. (2023) propose using STRIDE to design a secure HDMA and apply STRIDE to target specific threats and develop their HDMA design [12]. The STRIDE method is a threat modeling approach used for the structural analysis of system vulnerabilities and their consequences [13]. It is usually composed of a series of steps focused on three subtasks: (1) create a system abstraction by analyzing vulnerable assets, participating entities, and the trust barriers and relationships between them; (2) identify threats and their impacts according to the acronym against Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege; (3) devise countermeasures to address the threats [13,16]. STRIDE is proposed by Erler et al. (2023) because it is the most mature threat modeling method, provides a deep understanding of system-relevant vulnerabilities, and targets security properties such as integrity, availability, and confidentiality that are critical to HDMA [12]. Moreover, the analysis of the different trust relationships in step (1) of STRIDE influences the design decision factors of the proposed decision model. This is a deliberate decision to consider the encouragement of trust in a system through its conception and design, adding a focus on the needs and wishes of the system users (e.g., patients and healthcare professionals) while keeping those of the developer. Accordingly, STRIDE and the decision model should be embedded in a joint conceptualization process for future secure HDMA. We propose to perform the first subtask of creating the system abstraction with STRIDE before applying the decision model developed in this paper (see Section 4). The second and third subtasks can then optionally be carried out after applying the decision tree for detailed threat analysis. It is assumed that the developer has already chosen a Blockchain-based solution for their specific use case, as referenced in the earlier work of Erler et al. (2022) [10]. Accordingly, before applying the proposed decision model, whether a Blockchain-based solution is suitable for the specific use case should be verified. Details on the process to do so are to be found in the work of Wüst and Gervais (2018) [17]. Overall, the steps required in preparation for the application of the decision model are depicted in Figure 1.

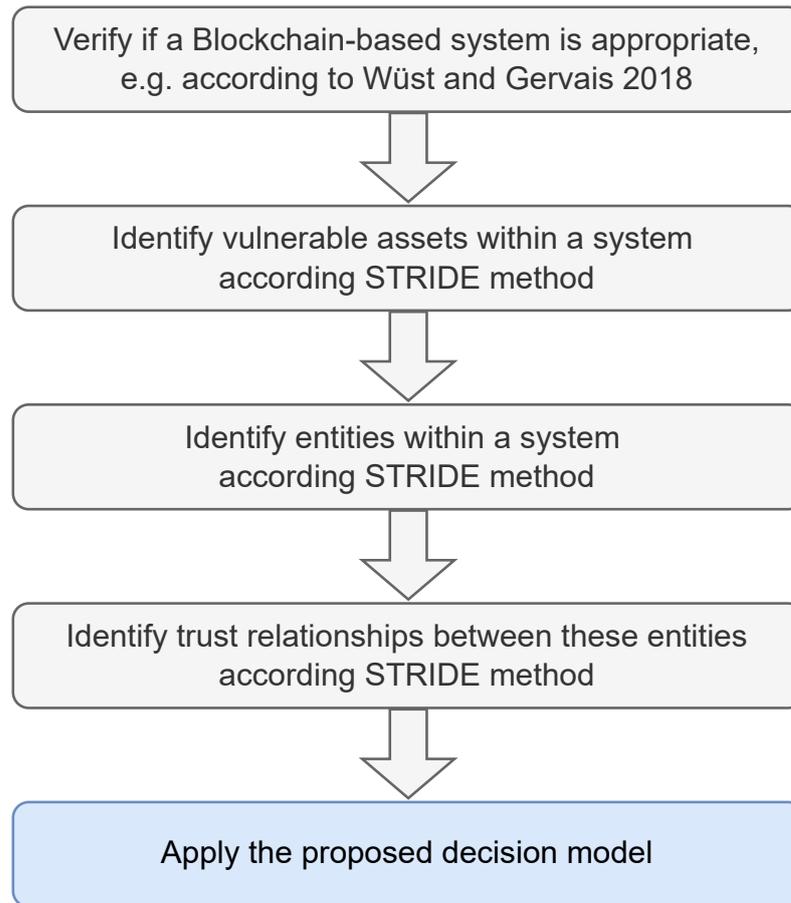


Figure 1. Steps in preparation of applying the proposed decision model, e.g. according to Wüst and Gervais 2028 [17] and STRIDE method [13,16].

2.1. Literature Review

The literature review conducted herein is based on the methodology found in Erler et al. (2022). In addition to their previous work, the importance of identity and access management in secure health data management systems is specifically addressed here. To do so, four scientific databases (ACM Digital Library, IEEE Xplore, EBSCOhost, and ScienceDirect) were searched in three iterations: Iteration one used identical search parameters as in [10]. Its purpose was to cover for retractions or corrigenda in the results since the search was conducted initially. Using the following search string yielded the same results as the original search in [10]:

(Blockchain OR distributed ledger) AND (sensitiv OR personal OR priva* OR confidential*) AND (data sharing OR data storage OR data exchange OR off-chain OR on-chain)*

These consisted of 19 proposed approaches from 18 papers, as found by Erler et al. in their 2022 literature review; no retractions or corrigenda were found.

To include more recent works, a second iteration was performed using the identical search string but limited to the time between 2022 and 31 December 2023. This resulted in identifying 13 new approaches, which were subsequently added to the taxonomy analysis. The third iteration of the literature search employed a different search string. This was conducted in order to cover identity and access management. It returned nine additional relevant publications:

(decentral OR "Blockchain" OR "distributed ledger") AND "identity" AND (health* OR medic*) AND ("data storage" OR "data donation" OR "access management")*

In total, 41 papers were found and reviewed. These include 18, as in Erler et al. (2022), from the first iteration of the search and 22 from the second and third iterations of the search. Erler et al.'s (2023) approach [10,12] was added to the results manually.

2.2. Taxonomy Development

Drawing inspiration from Erler et al. (2022) [10], we took the work of Nickerson et al. [15] as a guiding framework for developing our taxonomy. Nickerson et al. outlined a four-step process. The initial step involves identifying meta-characteristics, which serve as the foundation for deriving characteristics within the taxonomy. Second, they determine the termination conditions. In the third step, one of two approaches is applied: The first approach, "Empirical-to-Conceptual", involves analyzing objects for their shared characteristics. Objects are then organized according to their shared characteristics by grouping characteristics into dimensions. The second approach, "Conceptual-to-Empirical", conceptualizes objects' characteristics and associated dimensions. This third step is iterated until the termination conditions are met.

2.3. Approaches from Literature Review

Most approaches identified here aim to provide a decentralized Blockchain-based system to securely share sensitive health data between patients and care providers. In addition to this standard functionality, most approaches also cover extending the proposed networks to enable data sharing with the research community. Generally, and as for the structure of the approaches, all defer on data storage parameters (such as storage location and type), the type of general security measures taken, and how access control and identity are handled.

3. Taxonomy

In extension to Erler et al. (2022) [10], where they focused on data storage and data protection attributes, this work emphasizes identity and access management characteristics. Towards a complete taxonomy and to be consistent in methodology, we integrated the previously established dimensions and characteristics from the initial taxonomy development (see Section 3.1). Termination conditions were deemed satisfied when each dimension contained distinct characteristics and all necessary dimensions and characteristics required to classify all relevant objects were present. The classifications were conducted to the best of our abilities, as they had to be based on the information presented in the respective publications. More detail on the reasoning and the defining aspects of each dimension and their respective attributes can be found in the following Sections 3.1 and 3.2. As every paper we reviewed had a distinct focus, the description of the respective systems varied in the level of detail given to describe different aspects. Not every aspect of the systems depicted was clearly and thoroughly explained in every paper. In case of doubt or where descriptions lacked clarity or were devoid of specific taxonomy dimensions, we classified the respective approach in a more general manner or avoided classification. The resulting taxonomy with the assignment of the approaches to the dimensions we identified is shown in Tables 1–3.

Table 1. Taxonomy as resulting from the first search iteration.

| Search | Papers | Storage Location | Blockchain-Type | Off-Chain Storage | Encryption | Identity Management Type | Access Control Governance | Access Control Policy | NDAC logic | Access Granting Mechanism | Access Security Mechanism | Additional Storage Security |
|--------|-----------------------------------|------------------|----------------------|-------------------|------------|--------------------------|---------------------------|-----------------------|------------|--|--|-----------------------------|
| 1 | Li et al. 2018 [18] | Hybrid | public | centralized | hybrid | | | | | encrypted key exchange | public key encryption | hybrid encryption |
| 1 | Zhang and Lin 2018 [19] | on-chain | private + consortium | decentralized | asymmetric | | Data Owner | Hybrid | rule-based | search trapdoor exchange | public key encryption | asymmetric encryption |
| 1 | Hawig et al., 2019, App.1 [20] | on-chain | public | | symmetric | | Data Owner | DAC | | encrypted key exchange | public key encryption | symmetric encryption |
| 1 | Hawig et al., 2019, App.2 [20] | off-chain | public | distributed | symmetric | decentralized | Data Owner | DAC | | encrypted key exchange | public key encryption | symmetric encryption |
| 1 | Liu et al., 2018 [21] | off-chain | consortium | centralized | asymmetric | | Data Owner | DAC | | encrypted file location reference exchange | CP-ABE | symmetric encryption |
| 1 | Azaria et al., 2016 [22] | off-chain | private | decentralized | | decentralized (DTI) | Data Owner | DAC | | file exchange, query string | | |
| 1 | Zhang, White et al., 2018 [23] | off-chain | private | decentralized | asymmetric | decentralized | Data Owner | DAC | | encrypted file location | public key encryption | asymmetric encryption |
| 1 | Xiao et al., 2018 [24] | off-chain | private | decentralized | symmetric | decentralized | Data Owner | NDAC | role-based | encrypted file sharing, file location reference exchange, key exchange | | symmetric encryption |
| 1 | Chang et al., 2018 [25] | off-chain | public + consortium | decentralized | | decentralized (DTI) | Data Owner | Hybrid | rule-based | | | encryption n/s |
| 1 | Wang et al., 2019 [26] | off-chain | consortium | centralized | asymmetric | centralized | Data Owner | DAC | | encrypted file sharing | proxy re-encryption | asymmetric encryption |
| 1 | Dagher et al., 2018 [27] | off-chain | consortium | decentralized | hybrid | decentralized (SSI) | Shared | Hybrid | rule-based | encrypted key exchange, encrypted file location reference exchange | public key encryption, proxy re-encryption | symmetric encryption |
| 1 | Nguyen et al., 2019 [28] | off-chain | private | distributed | asymmetric | centralized | Data Owner | DAC | | file sharing | | asymmetric encryption |
| 1 | Hanley and Tewari, 2018 [29] | off-chain | private | decentralized | | decentralized (DTI) | Data Owner | DAC | | | | |
| 1 | Daraghmi et al., 2019 [30] | off-chain | consortium | decentralized | hybrid | decentralized (DTI) | Data Owner | Hybrid | rule-based | encrypted file location reference exchange | public key encryption, proxy re-encryption | symmetric encryption |
| 1 | Thwin and Vasupongayya, 2018 [31] | off-chain | private | centralized | asymmetric | centralized | Data Owner | DAC | | encrypted file exchange | proxy re-encryption | asymmetric encryption |
| 1 | Theodouli et al., 2018 [32] | off-chain | consortium | centralized | | centralized | Data Owner | DAC | | file location | | |
| 1 | Zaghloul et al., 2019 [33] | off-chain | public | centralized | hybrid | decentralized (DTI) | Shared | NDAC | rule-based | encrypted file exchange | CP-ABE | symmetric encryption |
| 1 | Zheng et al., 2018 [34] | off-chain | public | | symmetric | | System | NDAC | rule-based | encrypted key exchange | public key encryption | symmetric encryption |
| 1 | Zhou, Li, and Zhao, 2019 [35] | off-chain | public + consortium | distributed | hybrid | decentralized | Data Owner | DAC | | encrypted file exchange, encrypted key exchange | public key encryption, proxy re-encryption | asymmetric encryption |

Table 2. The taxonomy of the second and third search phases.

| Search | Papers | Storage Location | Blockchain-Type | Off-chain Storage | Encryption | Identity Management Type | Access Control Governance | Access Control Policy | NDAC logic | Access Granting Mechanism | Access Security Mechanism | Additional Storage Security |
|--------|-------------------------------------|------------------|----------------------|-------------------|------------|--------------------------|---------------------------|-----------------------|-----------------------|--|---|-----------------------------|
| 2 | Lee et al. 2022 [36] | off-chain | private | centralized | hybrid | | Data Owner | DAC | | encrypted file exchange/encrypted key exchange | public key encryption | symmetric encryption |
| 2 | Zhang et al., 2022 [37] | off-chain | consortium | centralized | hybrid | | Data Owner | NDAC | rule-based | encrypted file exchange | CP-ABE | symmetric encryption |
| 2 | Cao, Sun et al., 2021 [38] | off-chain | public + consortium | distributed | | decentralized (DTI) | Shared | Hybrid | rule-based | | | |
| 2 | Hu, Li et al., 2022 [39] | off-chain | | decentralized | | decentralized (DTI) | Data Owner | NDAC | role-based | query string exchange | | |
| 2 | Y. Wang, M. He, 2021 [40] | off-chain | private + consortium | centralized | | decentralized (DTI) | Data Owner | DAC | | | | encryption n/s |
| 2 | Jayasinghe, Shiranthaka et al. [41] | | | | asymmetric | decentralized (DTI) | | NDAC | role-based/rule-based | password protected file exchange | public key encryption + password protection | password protection |
| 2 | Lee et al. 2022 [42] | off-chain | consortium | distributed | asymmetric | decentralized (DTI) | Shared | NDAC | MAC | key exchange | proxy re-encryption | symmetric encryption |
| 2 | Zou, Lv et al., 2021 [43] | off-chain | public | decentralized | asymmetric | decentralized (DTI) | Data Owner | DAC | | encrypted file exchange | proxy re-encryption | asymmetric encryption |
| 2 | Nguyen, Pathirana et al., 2021 [44] | off-chain | private | distributed | symmetric | | | | | | | |
| 2 | Boumezbeur et al., 2021 [45] | off-chain | | centralized | hybrid | centralized | Data Owner | DAC | | encrypted key exchange | public key encryption | symmetric encryption |
| 2 | Gupta, Rodrigues et al., 2022 [46] | off-chain | public | distributed | | centralized | System | | | | | |
| 2 | Lin, Wang et al., 2022 [47] | off-chain | consortium | decentralized | asymmetric | decentralized (SSI) | System | DAC | | encrypted file exchange | proxy re-encryption | asymmetric encryption |
| 2 | E. Zaghoul, T. Li et al., 2022 [48] | off-chain | public | distributed | hybrid | decentralized (DTI) | Data Owner | NDAC | MAC/rule-based | encrypted key exchange | CP-ABE | symmetric encryption |
| 2 | Sabu, Ramalingam et al., 2021 [49] | off-chain | public | distributed | | centralized | Data Owner | DAC | | one-time-password exchange | | symmetric encryption |

Table 3. Complete taxonomy as result of search iterations 1 to 3.

| Search | Papers | Storage Location | Blockchain-Type | Off-chain Storage | Encryption | Identity Management Type | Access Control Governance | Access Control Policy | NDAC logic | Access Granting Mechanism | Access Security Mechanism | Additional Storage Security |
|--------|----------------------------------|------------------|------------------|-------------------|------------|--------------------------|---------------------------|-----------------------|------------|--|---------------------------|-----------------------------|
| 3 | Lee et al., 2020 [50] | off-chain | private | centralized | asymmetric | decentralized (SSI) | Data Owner | DAC | | encrypted file exchange | public key encryption | asymmetric encryption |
| 3 | Huang et al., 2020 [51] | off-chain | private | centralized | asymmetric | decentralized (SSI) | System | NDAC | role-based | encrypted file exchange | proxy re-encryption | asymmetric encryption |
| 3 | Zhao, Yu et al., 2022 [52] | off-chain | consortium | distributed | symmetric | decentralized (SSI) | Shared | Hybrid | role-based | key exchange | symmetric encryption | symmetric encryption |
| 3 | Li, Yue et al., 2021 [53] | Hybrid | consortium | distributed | symmetric | centralized | Shared | Hybrid | role-based | | | symmetric encryption |
| 3 | Ramesh, Mishra et al., 2023 [54] | off-chain | public | distributed | symmetric | centralized | | | | | | symmetric encryption |
| 3 | Qin, Jin et al., 2021 [55] | off-chain | consortium | centralized | asymmetric | centralized | Shared | DAC | | search trapdoor exchange and encrypted file exchange | proxy-re encryption | asymmetric encryption |
| 3 | Baldin, Chase et al., 2022 [56] | | | decentralized | | federated | Shared | NDAC | rule-based | | | encryption n/s |
| 3 | Lomotey, Kumi et al., 2022 [57] | off-chain | private | centralized | hybrid | centralized | Data Owner | Hybrid | rule-based | | public key encryption | symmetric encryption |
| 4 | Erler et al., 2023 [12] | off-chain | public + private | decentralized | | decentralized (SSI) | | DAC | | token exchange and file location reference exchange | | encryption n/s |

3.1. Existing Dimensions

The previously defined dimensions and characteristics of Erler et al. (2022) [10] were adopted into this work. There, storage location is defined as either on-chain, off-chain, or a hybrid approach. The Blockchain type can be public, private, or consortium and can be either permissioned or permissionless. In the case of off-chain storage, three different modalities are defined: decentralized, centralized, or distributed. The term “decentralized storage” refers to using existing infrastructure (i.e., servers) of participating care providers in contrast, while “centralized storage” implies dedicated infrastructure run by an entity legally and technically separate from care providers to store all data in one location. “Distributed storage” is considered as the splitting of data across different server nodes, as is performed with IPFS. Regarding the encryption used, the approaches found can also be sorted into the following dimensions: symmetric encryption, asymmetric encryption, and a hybrid version where both are used. A more detailed explanation of the dimensions denoted in this subsection can be found in Erler et al. (2022) [10].

3.2. Expanded Dimensions

The dimensions that go beyond the previously defined dimensions of Erler et al. (2022) [10] are explained in the following subsections.

3.2.1. Identity Management System

Some of the approaches we found do not clearly define where user identity information is stored or how a user’s access to his identity is managed [18–21,36,37]. Our taxonomy defines the different identity management systems based on where and under whose authority the user authentication secret is kept, based on Bouras et al. [58]. Centralized Identity Management systems store user information within a centralized storage location, which the service provider controls. User credentials needed for authentication—i.e., password and username—are stored there, allowing the service provider to restrict user access or fraudulently access user data. A user is, therefore, given little authority over their own information concerning the service providers. Federated identity management systems share an identity, which multiple service providers of a federation use. A user can authenticate himself with one of the federation’s partners and is automatically authenticated with all the others. This requires users to remember less authentication information and simplifies their interaction with these service providers. Each service provider of the federation maps the federated identity to their own identity for each user, stored within their own centralized storage location. Although the user profits from better usability, they are nonetheless granted no more authority over their identity than within the centralized identity management system. User-centric identity management systems can be combined with other identity management systems. The deciding factor that defines a user-centric identity management system is the personal authentication device (PAD). This device allows a user to authenticate himself locally with this device, which stores all the authentication information needed for different service providers. The authentication information is sent to the individual service providers upon successful authentication with the user-centric system. This system does not dictate how the user identity information is stored with each service provider and can, therefore, be applied to other forms of identity management systems. It can provide an extra layer of security by using biometric identity data like fingerprint or face recognition, which is stored locally on the PAD to ensure that simple authentication, such as usernames and passwords, cannot be used fraudulently. Decentralized Identity Management systems like decentralized trusted identity (DTI) or Self-sovereign Identity (SSI) use Blockchain technology to store and authenticate user identity. This means that storage of the key to proving one’s identity is decentralized, making it impossible for any single entity to delete it. A user receives a public and private key with which they identify or authenticate themselves. All authentication information is stored with the user and not controlled or entrusted to any third party. The key difference between DTI and SSI systems lies in the registration process. For DTI, registering a new

user depends on an existing third-party trusted identity, such as a government ID. The decentralized identity is, therefore, mapped to an existing one. For SSI, registering a new user is not dependent on any existing identity and, therefore, enables a higher level of anonymity than DTI [58].

Most decentralized trusted identity management approaches use an official government ID as their trusted third-party identity reference [22,25,38]. Hu and Li et al. (2022) generalize this third-party reference as a “real-world identity” [39], while Cao and Sun et al. (2021) specify a government or insurance ID [38]. Jayasinghe and Shiranthaka et al. propose using Amazon Recognition API to validate their use of Know-Your-Customer verification [41]. Huang et al. (2020) present an approach that mentions the registration of patients, hospitals, and research institutions using Hyperledger Fabric’s certificate authority [59], which in itself does not rely on a trusted identity reference and is, therefore, classified as an SSI approach [51]. Lee et al. (2022) mention that their certificate authority stores a mapping between the real-world identity and anonymous user identity keys within the Blockchain, rendering the identity system DTI [42]. Patients receive their own Blockchain address and personal Blockchain key pair after registering with the proposed SPChain of Zou et al. (2021) [43]. The registration transaction requires the patient’s medical record number, age, and other auxiliary information gathered at the first medical institution a patient visits when wanting to join the system. The institution’s medical record number is taken as the trusted third-party identification, rendering this type of Identity Management system DTI. Dagher et al. (2018) mention using a consensus verification process before adding medical and research institutions to the network [27]. However, patients are added with “little validation”, and only a numerical value is sent to voters within the consensus. The identity management systems are classified within this taxonomy from the patients only, rendering Dagher et al.’s approach as a decentralized SSI system. Zhang et al. (2022) differentiate between data owners, i.e., patients and data users, such as doctors or researchers. They mention that data owners need to register before using the system but only specify that data users are given private and public keys during registration. It is, therefore, unclear from the patient’s perspective what identity management system was used [37]. The approach of Ramesh et al. expresses that a patient receives a human-memorable password from the hospital, which seems to imply the creation of some sort of centralized account within the hospital system. They go on to mention a patient choosing their own secret key and generating their public key. The clear link between these two identities is not expressed, and a specific type of identity management system cannot be deduced. However, it is assumed that a centralized one is most likely [54]. The approach by Nguyen et al. gives the impression of utilizing a decentralized SSI approach. However, mentions of smart contracts being able to delete and add users, and the overall authority of who can trigger these contracts, remain unclear in their description [44].

According to our definitions, using a decentralized approach but storing the user’s private key in a centralized storage location of the overall service provider negates the user authority that the decentralized approach would grant. If a private key is not stored locally and independently by a user, the user gives up control over key usage and, therefore, gives control over the identity management to the service provider of the centralized storage location. Therefore, the use of Blockchain alone does not guarantee user authority. Storing the essential authentication information centrally effectively turns a decentralized approach into a centralized one.

It is important to note that many approaches derived from the papers we analyzed here do not go into detail regarding certain aspects of their design. The categorization is, therefore, performed to the best of our ability based on the information given. Boumezbeur et al. (2021) present a scheme in which a web portal is used as a “first level of security”. Here, a patient can log in using a username and password in order to see their basic medical information [45]. It is unclear how the generated keys used to interact and prove their identity within the Blockchain are stored. It is assumed that since such a portal exists, the administration of these keys is handled by the system providers. This provides usability advantages for the patients but negates the possible self-sovereignty the decentralized identity would be able

to provide. For instance, upon user registration through their frontend user interface flutter app, Gupta et al. (2022) produce a new empty wallet account on the Blockchain for their patient [46]. The patient is, therefore, given a sort of decentralized identity. However, the interactions with this wallet are strictly controlled by the hospital and can only be asked to be triggered by patients themselves. The authority over this wallet remains with the hospital. In essence, the account created on the mobile flutter app serves as the identity of the patient. As patients cannot control the mobile app, this identity system is centralized. Lee et al. (2020) propose a scheme that allows a patient to interact with other participants using a decentralized identity without mentioning additional identity references. They additionally offer patients a centralized account, allowing them to save the private key of their decentralized SSI identity within this account [50]. By giving patients this option, their approach is still classified as an SSI approach.

3.2.2. Access Control Governance

Approaches can be differentiated by which entity the data owner, i.e., the patient, the system, or a mixture of the two, has the authority to make access control decisions. Most systems presented here aim to give access control governance entirely to the data owner. Cao and Sun et al. (2021) distinguish between sensitive and non-sensitive data. Non-sensitive data are accessible to anyone, while control over access to sensitive health data remains with the respective users [38]. Here, the access control governance is shared between the system structure and the data owner because the system limits the access control decision-making of the patient. In Dagher et al. (2018), data owners can only execute limited access governance over their psychotherapy notes [27]. Similarly, Lee et al. (2022) limit their patient's sovereignty by issuing a re-encryption key to the doctor who created the data to allow access to the data in case a patient becomes unresponsive [42]. Huang et al. (2020) present an approach where the level of access to patient health data is determined by one of the pre-set roles a participant in the system is assigned to [51]. In this case, governance is completely determined by the system itself. Gupta et al. (2022) take a similar, rigid approach [46]. Lin and Wang et al. (2022) present a scheme that gives the hospital administrator the right to grant access to documents stored within their cloud, as all documents can be decrypted using the hospital's private key. Physiological information generated through a patient's phone, smartwatch, or private medical device is encrypted using the hospital's public key by the patients themselves before being uploaded into the hospital's cloud [47].

3.2.3. Access Control Policy

Access control policies can be categorized into either Discretionary Access Control (DAC), where access control is executed on the level of individual entities in the system, or into Non-Discretionary Access Control (NDAC) (or a hybrid of the two). NDAC can be seen as a more coarse way to assign access, using rules or logic to form the necessary abstraction from individual entities [60]. Another concept found in [60,61] is Mandatory Access Control (MAC). Here, each file and each user are assigned "levels". Only if a user's level is equal to or higher than that of the file to be accessed will access be granted. Role-based Access Control (Role-BAC) defines a user's access based on their assigned role within the system. It can be understood as a sub-variant of NDAC. Another broadly defined access control variant is Rule-Based Access Control (Rule-BAC), where access is assigned by rules. This includes Attribute-Based Access Control [60,61]. Lee et al. (2022) and Zaghloul et al. (2022) are two of the few approaches using MAC as their access policy logic [42,48]. Most others rely on a general rule-based access control policy.

3.2.4. Access Granting Mechanism

The approaches under consideration herein can be differentiated by the mechanism used to enable access to a resource. In its simplest form, access is gained by transferring the resource directly to the recipient, a concept found in Nguyen et al. [28]. Refs. [31,33] describe

a similar concept, where an encrypted file is transferred that can be decrypted by recipients using their own private key. Others describe the exchange of an encrypted key that can be used to decrypt the desired file [18,20,34,35]. Another variant of granting access is by using references, as found in [19,22], where a search trapdoor or data query string is used. Similarly, Liu et al. describe the exchange of an encrypted file location reference [21]. Lee et al. (2022) describe a method to grant access to documents by issuing a re-encryption key and having the recipient re-encrypt the encrypted file they receive and decrypt it using their private key. The recipient acts as the proxy entity itself in this case. Using this method, the mechanism is the re-encryption key, and securing this transfer is proxy-re-encryption [42]. Sabu et al. (2021) simply exchange a one-time password to the access-receiving doctor [49].

4. Resulting Decision Model

Figure 2 shows the proposed decision model. Its characteristics regarding Blockchain type, data storage locations, and off-chain storage have been adopted from Erler et al.'s previous publication [10]. Building on their work, decision factors were modified to take trust between actors in the system into account. Therefore, for the identified dimensions, the four questions of Erler et al. for the design of Blockchain-based HDMA [10] were supplemented and extended by six additional questions, which are described below.

4.1. What Type of Blockchain should Be Used?

See Figure 2. The selection of a Blockchain type for an HDMA primarily depends on whether it will be administered and supervised in a decentralized manner (e.g., by a single healthcare provider) or collectively by multiple providers. Public Blockchains are well-suited for decentralized systems that do not depend on any specific provider [10]. These Blockchains are accessible to anyone willing to join and do not restrict access. In contrast, private Blockchains are well-suited for systems overseen by a solitary healthcare provider or a government institution, while consortium Blockchains are a suitable choice for systems managed by multiple healthcare providers [10]. Access to these Blockchains can be restricted by these supervising entities to only relevant system participants. This reserves power within the overall system to these single entities. However, in certain scenarios, the use of multiple Blockchains can prove advantageous. To detect any potential tampering with private or consortium Blockchains by the responsible entities, their transactions can be cross-referenced with other Blockchains. Additionally, dispersing data across multiple private Blockchains can help address scalability issues associated with on-chain storage [10].

4.2. Which Storage Type should Be Used?

See Figure 3. Healthcare data can be stored on-chain. In this case, however, the amount of data stored on a Blockchain is often limited by maximum transaction and block sizes [3]. Generally, it is advisable to store data smaller than its hash value on the Blockchain and larger data off-chain [3]. A hybrid approach allows meta-data, like the hash of the data, to be stored on Blockchain to be able to profit from its immutability while having most data stored off-chain [3,10]. Generally, many healthcare providers are hesitant to share their data [12]. If there is no trust in the system storage, off-chain storage should be chosen.

4.3. Which Off-Chain Storage Is Suitable for Storing Data off the Actual Ledger?

See Figure 3. Healthcare data can be stored in a decentralized, centralized, or distributed fashion. Healthcare providers may be hesitant to make the data stored within their secured infrastructure available to an external system. However, the cooperation of healthcare providers in such a system is essential. In case of a lack of trust from participating healthcare providers, leaving stored data within their original healthcare provider's storage locations in a decentralized manner would be the best option. However, if healthcare providers are willing to place their data elsewhere and a single entity is trusted with said storage, a centralized storage solution can be chosen, such as a cloud server. If no single entity is trusted, data can either be stored locally with each patient, which would entail a large

technical burden on the patient's side, or in a distributed fashion, like an InterPlanetary File System (IPFS).

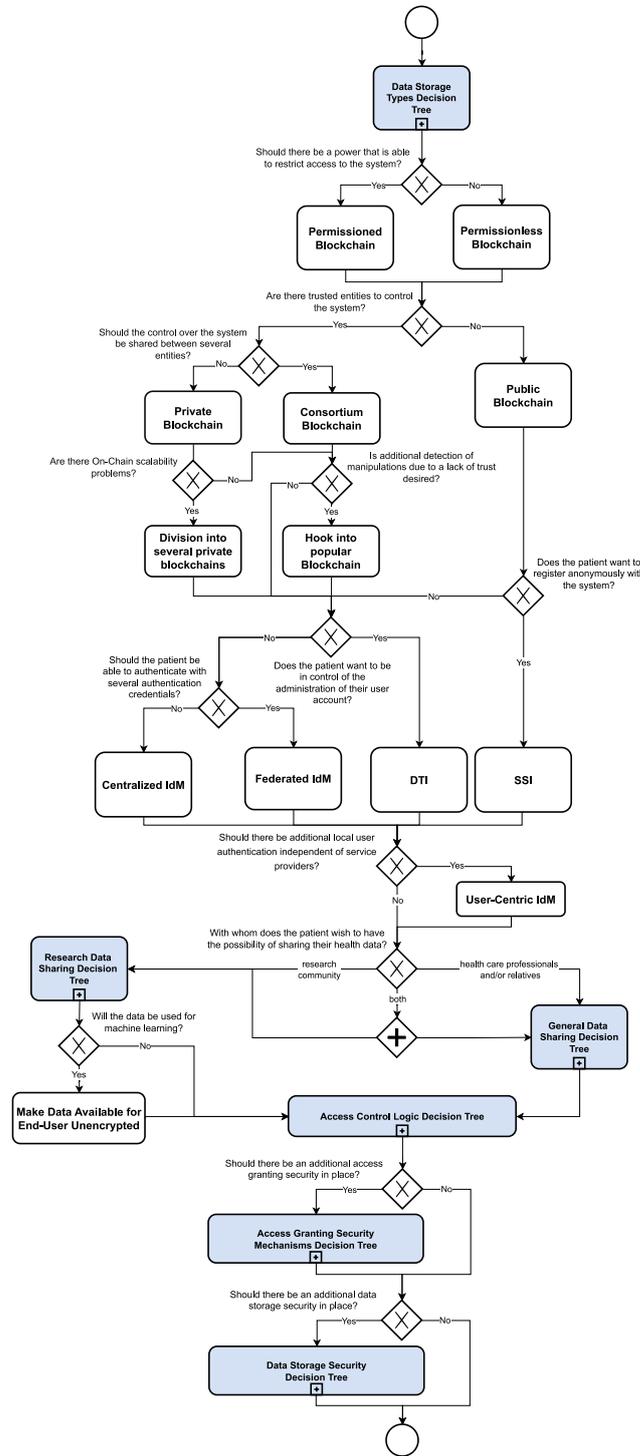


Figure 2. The resulting decision model.

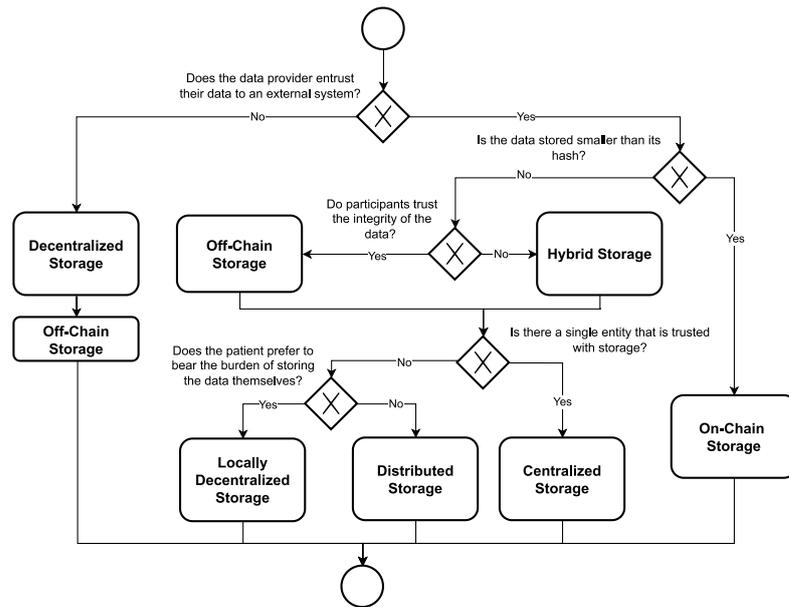


Figure 3. The data storage types sub-decision model.

4.4. What Identity Management System should Be Used?

See Figure 2. Selecting the appropriate identity management system is a crucial decision for any organization, given its potential impact on the security, usability, and self-determination of users. Identity management can be categorized into distinct types: centralized, federated, user-centric, and decentralized. Within the decentralized category, there are two subtypes: Self-sovereign Identity systems and Decentralized Trusted Identity (DTI) systems. Decentrally stored user identities are exemplified by decentral identity management systems like DTI and SSI. User identities are saved on a Blockchain rather than a centralized server and are, therefore, not controlled by one entity. SSI and DTI differ in their registration method. Self-sovereign Identity allows users to join a system with complete anonymity, while during user registration, a decentralized trusted identity depends on the identity reference of a trusted third party for each new user. The benefit of pure anonymity is, however, negated if SSI is applied to a private or consortium Blockchain, which can restrict and, therefore, filter access based on its own criteria. Centralized and federated identity management systems store user identity centrally on their servers controlled by the service provider. Centralized identity management systems are particularly valuable for organizations with a large user base, but they do not allow users to execute ownership over their identities. These systems are widely used, requiring users to create new accounts for each centralized system and manage an ever-expanding array of distinct credentials. On the other hand, federated systems offer a slightly improved user experience by offering easier authentication through mappings of shared authentication credentials. By allowing an extra layer of authentication through a personal authentication device, any of the aforementioned identity management systems would be gaining the functionality of a user-centric identity management system.

4.5. With Whom Does the Patient Wish to Share Their Health Data?

See Figures 4 and 5. Depending on the patient’s willingness to share their data, a system could allow general healthcare data to be exchanged amongst healthcare providers and relatives, and/or to the benefit of research institutes. For each of these groups, an access governance and access logic need to be chosen.

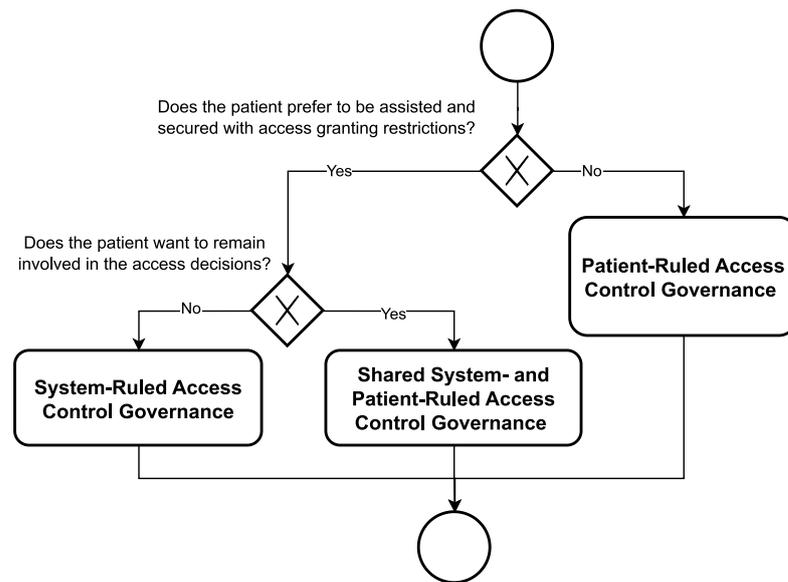


Figure 4. The general data sharing sub-decision model.

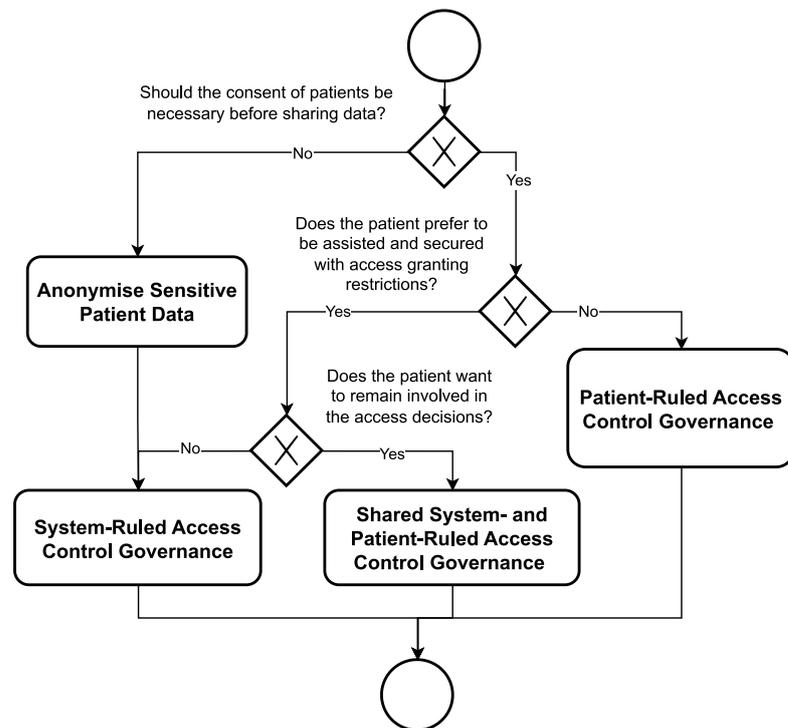


Figure 5. The research data sharing sub-decision model.

4.6. Is Data Being Used for Machine Learning?

See Figure 2. In the case of sharing health data with the research community, Erlar et al. point out that shared data need to be unencrypted when given to potential end users to allow for the effective application of machine learning technology [10]. This was adopted into this decision model.

4.7. Who should Govern the Data Access Strategy?

See Figure 6. Empowering the system to control the data access strategy requires a well-thought-out and thoroughly tested approach that universally safeguards data owners from their own errors or uninformed actions. Nonetheless, this approach removes decision-making authority from the data owner, depriving them of the ability to self-govern their

personal data. On the other hand, granting the data owner exclusive control over the data access strategy enables them to take ownership of their data. However, this approach comes with the risk of unintentionally permitting malicious access by external parties. A balanced approach, which allows the system to impose some restrictions and oversight while still giving the data owner a degree of self-governance, can offer a more secure user experience.

In terms of sharing data with the research community, the need for patients to give consent to the use of their data can be avoided by anonymizing the respective data. In this case, the system can be in charge of all access governance.

4.8. What Access Policy should Be Used?

See Figure 6. Discretionary access control (DAC) provides a means for detailed Access Management and straightforward monitoring but imposes significant administrative workload on the entity responsible for access control, whether it be the system, data owner, or both. In contrast, Non-Discretionary (NDAC) access control streamlines Access Management, reducing the administrative burden, albeit potentially resulting in less granularity in access control. In certain situations, a hybrid approach might offer greater flexibility, although it is essential to note that exploiting access policy loopholes could introduce security vulnerabilities to the system.

4.9. What Additional Access Granting Security should Be Used?

See Figure 7. Enhanced access security measures may ensure that the entity or individual who was granted access to a resource is indeed the intended recipient. To provide access in its most basic form, permission could be granted by providing the symmetric key used for resource encryption. This approach does not tie access security to a particular recipient, and the same key can be issued to multiple entities. Any entity possessing this key could access the encrypted resource. If access needs to be associated with a specific recipient or with a specific group of recipients, the intended recipients may be defined based on attributes they possess or individually.

Cipher policy attribute-based encryption allows entities with the necessary attributes to access a resource, enabling access for a broader group. However, it necessitates the presence of an access policy before granting access, limiting its flexibility. Access security with individually defined recipients can incorporate a specific identity locked into the security mechanism or remain identity-agnostic.

Tokenization ensures that only the specific individual holding the token can access a resource. Tokens are distributed on an individual basis, with each entity receiving one token. The holder of this token can provide a digital signature when submitting it, allowing the system to verify the recipient's identity before granting access. However, the tokenization method itself does not specify the specific identity of the holder.

To link access security to a specific identity, a public and private key pair of an entity is employed. Through asymmetric encryption, only the recipient possessing the intended identity (private key) can gain access to a resource. When sensitive data are stored in an untrustworthy location, proxy re-encryption permits a data owner to grant access to a specific identity by issuing a re-encryption key. This key enables a potentially untrustworthy data storage location to re-encrypt the already encrypted data without exposing it, allowing the recipient's private key to decrypt it. In cases where data are stored in a trustworthy location, simple public key encryption is sufficient to secure access for a specific identity holder.

4.10. What Additional Data Storage Security should Be Used?

See Figure 8. Data can be safeguarded through encryption or password protection. While password protection offers some level of security, it falls short in comparison to encryption [62]. Encryption can be broadly categorized into two types: symmetric and asymmetric. Asymmetric encryption provides more robust security as it necessitates two distinct keys for encryption and decryption. However, this encryption method demands more resources and is practical, mainly for smaller files like text documents. Symmetric

encryption is better suited for encrypting larger files due to its efficiency in the encryption process. Nevertheless, it is considered less secure. A practical approach involves using symmetric encryption to encrypt the files themselves and then encrypting the symmetric key with asymmetric encryption. This hybrid encryption strategy combines the strengths of both encryption types, enabling secure encryption while maintaining efficiency and minimizing the risk of key exposure.

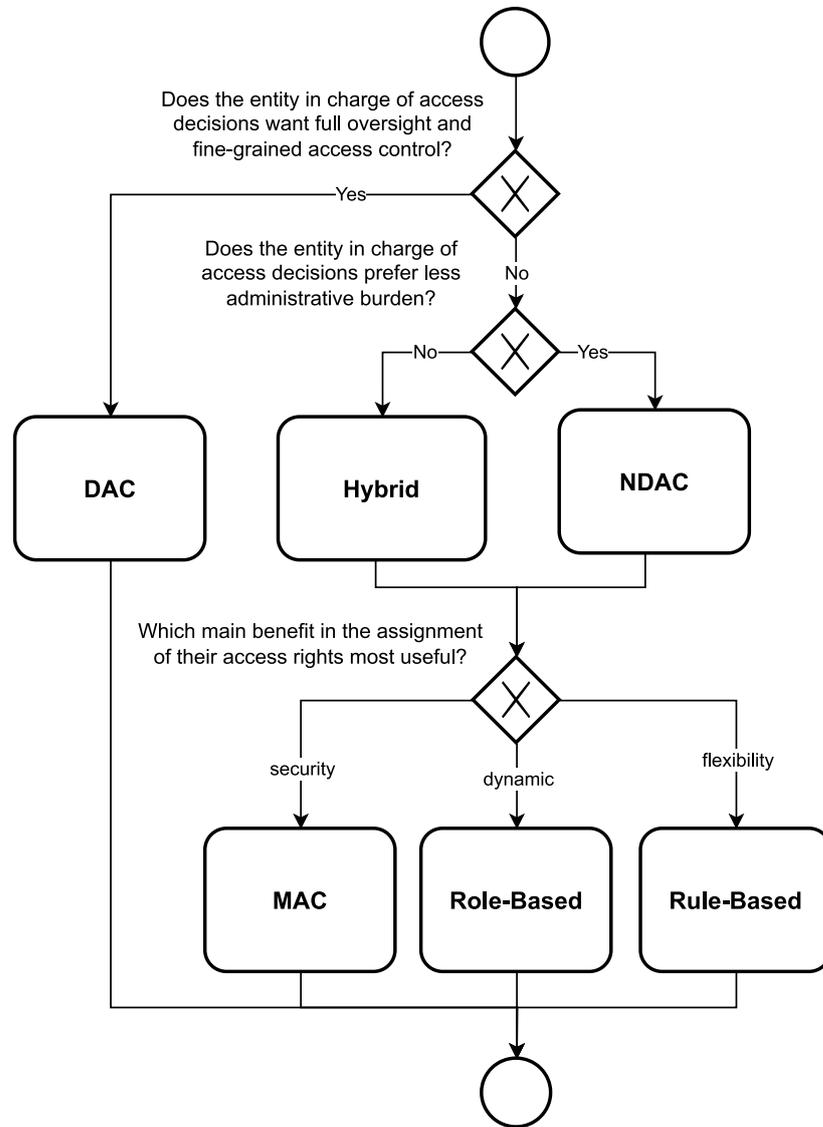


Figure 6. The access control logic sub-decision model.

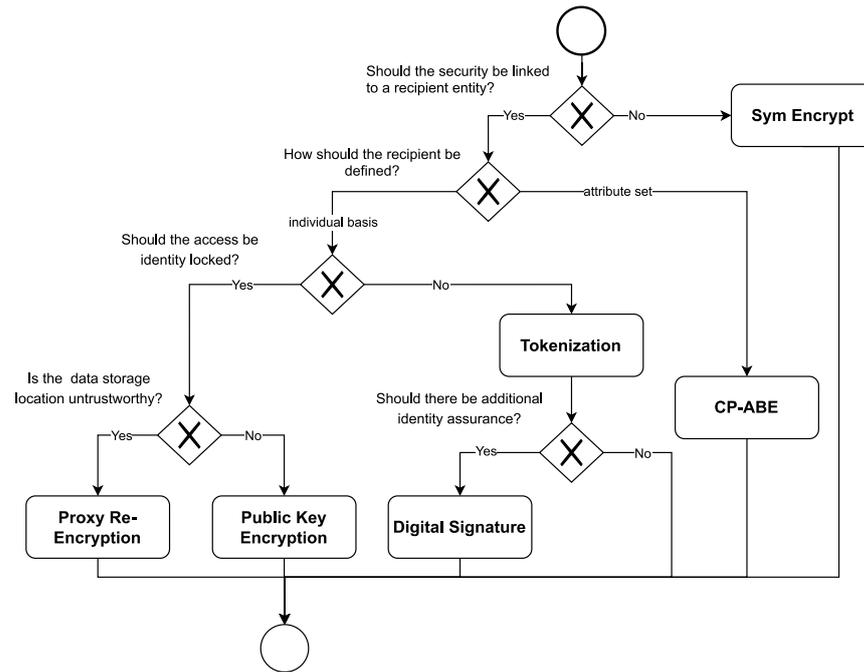


Figure 7. The access granting security sub-decision model.

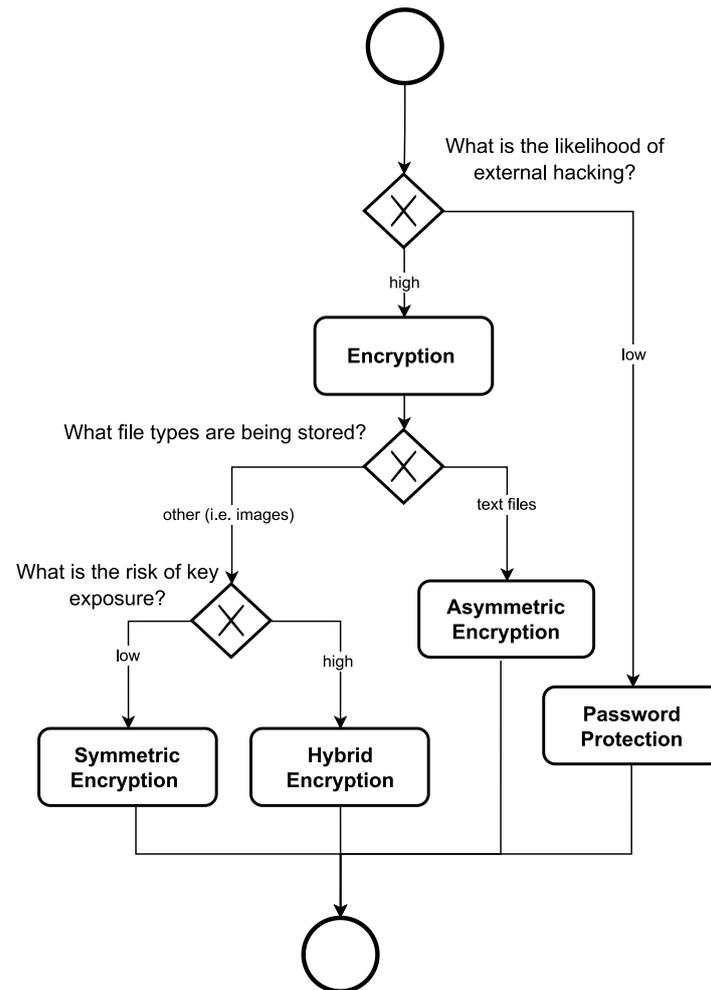


Figure 8. The data storage security sub-decision model.

5. Evaluation

In this section, we evaluate the resulting decision model from Section 4 by first discussing it with experts from different areas of expertise and second by applying it to the three specific use cases: (1) management of data from a digital dementia screening application; (2) general health data management application in medical care; (3) data donation via a data trustee for secondary use of the data for medical research and development. These use cases were chosen for the following reasons: First, the three use cases each represent different relevant scenarios for sharing health data, namely, the integration and sharing of health data from digital health applications via a personal health record (PHR), the management of data from healthcare providers, and the donation of the entire health data for secondary use by research and development. This means that the use cases cover most of the relevant entity constellations in healthcare. In addition, the first use case was already applied to the existing decision model of Erler et al. [10] and a concept was derived, which can be used to check whether the same concept results with the decision model extended in this work.

To validate the decision tree, a two-hour online expert workshop was held with an expert group, which consisted of seven experts from the field of research in computer science and information security. Four of the seven experts have particular experience with the realization of Blockchain projects, either from a conceptual or technological point of view. The remaining experts are more concerned with the area of de-identification and quality of health data for secondary use. As part of the expert workshop, the decision tree was first presented, and its application was demonstrated using use case (2). The experts were then able to ask questions and give comments on the decision tree in an open discussion. The criteria for evaluating the decision model were completeness, consistency, and actuality. In addition, the design decisions for the German healthcare system were discussed. However, we do not provide specific metrics or guidelines for evaluation.

This feedback was then incorporated to adjust the decision tree. The second part of the evaluation is described below using the three use cases. The resulting design characteristics for the systems in the use cases resulting from the application of the decision model are summarized in Table 4.

5.1. Use-Case 1: Management of Data from a Digital Dementia Screening Application

By applying the resulting decision model depicted in this paper to the proposed design plan for DemPredict, as published by Erler et al. (2022) [10], the same design choices are expected. The decision model leads to the selection of a permissioned Consortium Blockchain and off-chain Distributed Storage on IPFS because the data are larger than its hash value and should be deletable. By choosing a Consortium Blockchain operated by multiple organizations, the operator of DemPredict entrusts the storage of the data to external systems and several entities should share power to restrict access to the system. According to Erler et al. (2022) [10], trust in third parties is not always given. Accordingly, it is assumed through the Hybrid storage approach (off-chain storage of the data in IPFS and on-chain storage of the hash of the data) that the integrity of the data is not trusted, and there is no single entity that is trusted with the storage. If the state were to be trusted as a single party to store the data, a central storage would be conceivable, but according to the authors, this is not the case. It is assumed that the data subjects do not want to bear the burden of data storage themselves in terms of usability. In addition, no scalability problems and no additional detection of manipulations are required. Accordingly, the decision model proposed in this work comes to the same decisions regarding data storage and Blockchain type. No statements are made by Erler et al. (2022) [10] regarding identity management, so no reliable statements regarding this topic can be made. However, based on the intended approach of a PHR, one can assume that the data subject wants to make self-sovereign decisions about their own data and wants to manage their user account themselves. If this were the case, a DTI approach with user-centric IdM would be conceivable according to the proposed decision model. The data subject wishes to share his data with the research community and healthcare providers. According to Erler et al. (2022) [10], when personal

data, particularly personal health data, is being utilized for medical research, it should be anonymized or pseudonymized to ensure compliance with data protection regulations and safeguard the privacy of individuals. Accordingly, two paths are possible in the research data sharing sub-decision model (see Figure 5), both of which, however, can result in system-ruled access control governance. The research data will not be used for machine learning and can be stored encrypted. Regarding the sharing of data with other healthcare professionals, a shared system- and patient-ruled access control governance is proposed by the decision model because the patient prefers to be assisted with access granting restrictions for usability reasons and also would like to be included in the access decisions with a simple fine-grained DAC logic (ACL). In addition, the system provider can be seen as a trustworthy oracle and can be involved in access governance. For data protection purposes, Erler et al. (2022) [10] symmetrically encrypted the data. Accordingly, additional data storage security is desired, and the security should be linked to a recipient entity. Overall, the same design decisions made by Erler et al. (2022) using their decision model can be made for this use case using our proposed decision model.

5.2. Use-Case 2: General Health Data Management Application in Medical Care

The decision model leads to the use of off-chain decentralized storage, which Erler et al. (2023) [12] propose using as well because the data remain within the systems of the data provider and no external system needs to be trusted. The protection mechanism PM27 of Erler et al. (2023) [12] suggests the use of a permissioned Blockchain to restrict access to the Blockchain network. However, there is no trusted entity to control the system and manage the identities, which is why a Public Blockchain would be suitable. In accordance with PM1, personal registration or authentication should take place at a technical level. By using an anonymous credential via SSI, the patient can remain anonymous and still register and connect with his medical institutions. In addition, local user authentication is desired to secure the credential wallet using a password (PM5 of Erler et al. (2023) [12]). Therefore, a User-Centric IdM is used. Overall, the aim of the work proposed by Erler et al. (2023) [12] is to share data with healthcare professionals and relatives under the full control of the patient, but not with researchers. Accordingly, a patient-controlled access governance through fine-grained DAC logic is proposed by the decision model. Additional access granting security should be in place to grant specific data consumers individual access to the data. Therefore, tokenization combined with digital signatures is used by Erler et al. (2023) [12] as part of the implemented DIDComm Network Communication and proposed by the decision model. Additional data storage security inside of the internal systems of the medical institutions should be in place via data encryption according to PM 16 of Erler et al. (2023) [12]. As all types of health data are stored and the risk of key exposure is low due to secure management within the medical institutions and exclusive use of the keys within the medical institutions, the data itself should be secured using symmetric encryption. Similarly, the proposed system design of Erler et al. (2023) [12] can also be achieved by applying our decision model.

5.3. Use-Case 3: Data Donation via a Data Trustee for Secondary Use of the Data for Medical Research and Development

In the following, the decision model will be evaluated by considering the requirements of a data trustee system by Schinle et al. [63]. Afterwards, a system concept for such a data trustee is proposed. It is assumed that the health data providers prefer to keep their data within their own internal storage locations and provide them to the data trustee if needed, similar to Erler et al. (2023) [12]. Therefore, health data should be stored off-chain and decentralized. As sensitive health data are to be exchanged, access to the system should be restricted and a permissioned Blockchain should be used accordingly. In order to create trust and transparency, no trusted entity should be required to control the Blockchain network, and a public Blockchain is, therefore, a suitable option. To create trust and transparency (S4, S2.2, and S2.3 from Schinle et al. [63]), no entity to control the Blockchain network should be needed. A Public Blockchain is, therefore, a suitable option. Through the use of pseudonymization, monitoring of longitudinal data is made possible but requires the secure administration of the identity of the data subject himself and the possibility of registering anonymously under a pseudonym (S3.3 from Schinle et al. [63]). This leads to the use of SSI as the identity management system. Furthermore, no extra local user authentication is necessary. The systems aim to allow the sharing of data with select healthcare providers and relatives (S1 from Schinle et al. [63]) as well as with the research community and third parties (S1.1 from Schinle et al. [63]). In the case of research data sharing and general data sharing, a patient-ruled access control governance is chosen in order to allow the patient full and unlimited control with whom they wish to share their data (S2 from Schinle et al. [63]). Beyond that, the subject's data may only be processed and shared if consent has been obtained (S2.1, S3, and S4.1 from Schinle et al. [63]). The access logic to support this governance structure is DAC in charge of full oversight and fine-granted access control (T1.4 from Schinle et al. [63]). The data should be used for machine learning. T1.3 from Schinle et al. [63] proposes, therefore, to use privacy-preserving analytics with encrypted data but is limited to algorithm training and does not include explorative analysis. Accordingly, the data should be encrypted if privacy-preserving analysis can be applied and not provided encrypted if it cannot be applied. In order to enable access from being granted, public-key encryption is used to ensure that the correct end-user is given access on an individual basis. The stored data, which resides in this design on external decentralized storage locations of the participating healthcare providers, could be protected using simple symmetric encryption due to the size of the data. However, since the data are stored externally from the system, the administration and security fall under the control of the trusted various healthcare providers, and its storage location protection is not a responsibility or a decision that befalls the system itself (T2.1 from Schinle et al. [63]).

From the design decisions described above and the proposed design of Erler et al. (2023) [12], the data trustee system concept illustrated in Figure 9 can be derived. By using the modern DIDComm standard (<https://identity.foundation/didcomm-messaging/spec/>, (accessed on 5 April 2024)) for decentralized and trustworthy data exchange between the medical institutions and the data trustee system, data subjects gain unified access to their scattered health data and the ability to autonomously decide on data donation, without primarily granting additional central intermediaries access to the data. In the web app, data subjects can connect with data-generating and providing medical institutions, view descriptions of their stored health data, and give consent to use the data for research. The storage of this health data, including corresponding consent and sharing rules, continues to be decentralized in the existing internal systems at the data-providing medical institutions. The connector allows this information to be made accessible to data-providing medical institutions through the network infrastructure of the data trustee web app. However, interfaces are needed to identify the data for which consent is present. This occurs during the data subject's onboarding at the medical institution. The data subject can connect with the medical institution using the web app and prove their identity physically and technically on-site. Then, the data subject's study pseudonym is stored in the institution's

connector along with the research pseudonym of the data trustee. The data subject can then decide on data donation. Communication and data exchange between data-generating and -providing medical institutions, as well as the data trustee system, take place through the network infrastructure, a decentralized, Blockchain-secured network for peer-to-peer (P2P) communication. The network complies with the modern open-source standard DIDComm and is based on the open-source implementations Ursa, Indy, and Aries of the Hyperledger Foundation (<https://www.hyperledger.org/>, (accessed on 5 April 2024)). Hyperledger Indy (<https://www.hyperledger.org/projects/hyperledger-indy>, (accessed on 5 April 2024)) is a permissioned public Blockchain framework for SSI. Communication within the network infrastructure occurs through the decentralized P2P DIDComm network consisting of Aries Agents (<https://github.com/hyperledger/aries>, (accessed on 5 April 2024)). Mediator agents (<https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0046-mediators-and-relays/README.md>, (accessed on 5 April 2024)) enable asynchronous, encrypted communication between the web app and connectors. The DIDComm network is complemented by an identity Blockchain, which serves as a trust anchor for network participants. The Blockchain publishes a tamper-proof directory for digital signatures and network addresses, enabling trustworthy communication based on verified digital identities for data-generating and providing medical institutions and the data trustee system. The identities used are exclusively for communication within the network and are separate from identities within the data-generating medical institutions and pseudonyms in the data trustee system. The partially identifying user data of the data trustee system itself (e.g., user email addresses) are stored in a separate database of the data trustee and are not automatically linked to clinical or research data, unlike the stored decisions. Once the linking and establishment of a P2P connection between medical institutions and the data trustee system, as well as consent for data usage, have been completed, data users can request data availability via their web app. They can define research-relevant criteria (inclusion and exclusion criteria) for the required data and provide information about their research project and objectives in advance in order to be authorized for system usage by a legal representative via their web application. The request is then forwarded to the linked connectors, and an automated comparison of usage intentions with existing consents is carried out. If there is a positive match, an aggregated response of the available data sets from all connectors is initially forwarded to the data user via the data trustee connector. Based on this, the data user can conclude a usage agreement with the data trustee system. Upon approval, the data are provided to the data user in pseudonymized form within the trusted execution environment for data trustee experiments. In this environment, they can upload and execute their algorithms and experiments. Auditing all accesses and processing steps within such experiments through a logging Blockchain enables control over the legality of data usage. Reviewers can subsequently validate the logged information via the tamper-proof Blockchain. Dedicated separate web servers are operated for the web application of the data-providing institutions and those of the other stakeholders within the data trustee system. In addition, the data trustee system provides for the integration of a data quality pipeline, which is maintained by a technical IT system administrator of the data trustee and managed with quality-enhancing services.

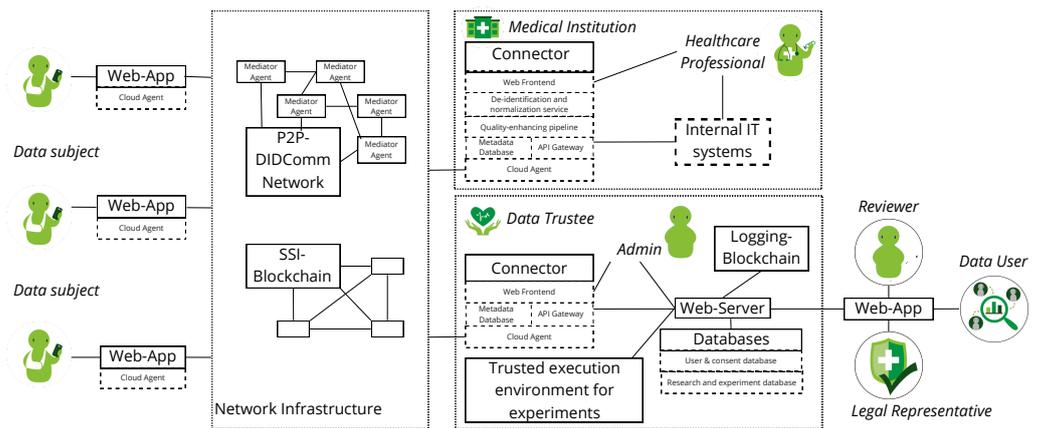


Figure 9. Proposed system concept for the data trustee system to support data donation.

6. Discussion

The design of HDMA and the associated data ecosystems based on Blockchains for exchanging, managing, and storing particularly sensitive health data is a complex undertaking. A large number of design decisions have to be made in order to take into account the diverse needs and trust assumptions of all stakeholders. Especially with regard to Blockchain-based applications, it is important to carefully examine whether the use of this technology serves a purpose. A Blockchain should be seen as a complementary tool that can provide added value if its properties of decentralization, transparency, and immutability are key to a given project. In particular, the topic of access and identity management with Blockchain needs to be taken into account early in its conception. It has so far been neglected in existing models. To be able to do so, a comprehensive decision model that facilitates the choice of an appropriate design based on a prior stakeholder and security analysis is needed. Any such decision model must incorporate a realistic assessment of the trust relationships between all actors as well as a strong focus on identity and access management. Only by using such an approach can a useful multi-contribution Blockchain-based HDMA be designed. To develop a decision model that satisfies these requirements and in order to support system architects and developers in the design process, a methodical approach was proposed (see Section 2). A structured literature search was then used to identify the state of the art regarding existing designs and technical implementations for Blockchain-based HDMA. The findings of this search were then incorporated into an iterative taxonomy development process. The taxonomy developed has assisted in summarizing the technical features of existing Blockchain-based HDMA, thereby identifying the key junctures where design decisions need to be made (see Section 3). The basis for this was provided by the existing method and taxonomy by Erler et al. (2022) [10]. Following this, the resulting taxonomy was used as a tool to construct the decision model (see Section 4). Overall, the decision model aims to expand the already published explorations of Erler et al. (2022) [10] and Xu et al. (2021) [11]. It was able to include identity and access management as a design feature as well as address concerns of trust, analyzed using the STRIDE method [13]. To the best of our knowledge, we have conducted the literature review and the development of the taxonomy as the basis for the development of the decision tree. Nevertheless, existing approaches could have been unconsidered because the resources for the literature search were limited and only related to the defined search string. The timeliness of the decision tree, as well as examining the extension of the decision to other areas of application, would also be possible directions for future work. Through the evaluation, the applicability of the decision tree in the three use cases was demonstrated and initial expert feedback was obtained via the expert workshop. Due to the limited time, open design of the workshop, and the low diversity of the expert group, we would like to emphasize that the feedback received from this is limited. Accordingly, a comprehensive survey with a specific interview guideline and a diverse group of experts would be a possible next step. However, the three

use cases made it possible to cover a broad spectrum in the area of health data management and to develop a decision model specific to this area. Overall, the decision model is able to guide design decisions of all three use cases. It is able to address trust relationships as well as system developer needs. In particular, in use case (3), not only was an existing design evaluated with regard to the same design decisions, but a new system concept for a data trustee was derived and presented (see (3) in Section 5). Future work should include a more detailed analysis of the technical aspects of providing data securely through a data trustee. The literature so far has been sparse when it comes to describing the technical structure or design of a data trustee. In addition, a prototypical implementation of the use case concepts would be useful in evaluating their practical applicability. Another essential aspect that was identified as relevant during the literature research, particularly in the conception of decentralized and distributed HDMA, is the integration of (privacy-preserving) machine learning approaches, which are only addressed to a limited extent in the current literature and the proposed decision tree. With regard to this aspect, future investigations and additions to the decision tree would be conceivable.

Author Contributions: Conceptualization, C.E. and A.-M.B.; methodology, C.E. and A.-M.B.; validation, C.E. and A.-M.B.; Investigation, C.E., A.-M.B. and F.G.; Resources, C.E. and A.-M.B.; Writing—original draft, C.E. and A.-M.B.; Writing—review and editing, C.E., A.-M.B., F.G. and W.S.; Visualization, C.E. and A.-M.B.; Supervision, W.S.; Project administration, C.E., F.G. and W.S.; Funding acquisition, C.E. and F.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the German Federal Ministry of Education and Research (BMBF) within the research project SouveMed under the grant number 16DTM115A.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author/s.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ismail, L.; Materwala, H.; Karduck, A.P.; Adem, A. Requirements of health data management systems for biomedical care and research: Scoping review. *J. Med. Internet Res.* **2020**, *22*, e17508. [CrossRef] [PubMed]
2. Pohlmann, S.; Kunz, A.; Ose, D.; Winkler, E.C.; Brandner, A.; Poss-Doering, R.; Szecsenyi, J.; Wensing, M. Digitalizing health services by implementing a personal electronic health record in Germany: Qualitative analysis of fundamental prerequisites from the perspective of selected experts. *J. Med. Internet Res.* **2020**, *22*, e15102. [CrossRef] [PubMed]
3. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*, 1st ed.; Springer Nature: Cham, Switzerland, 2019.
4. Häyrynen, K.; Saranto, K.; Nykänen, P. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *Int. J. Med. Inform.* **2008**, *77*, 291–304. [CrossRef]
5. Richter, G.; Borzikowsky, C.; Hoyer, B.F.; Laudes, M.; Krawczak, M. Secondary research use of personal medical data: Patient attitudes towards data donation. *BMC Med. Ethics* **2021**, *22*, 164. [CrossRef] [PubMed]
6. Arlinghaus, T.; Kus, K.; Kajüter, P.; Teuteberg, F. Designing Data Trustees: Status quo and Perspectives for Business Models. *HMD Praxis der Wirtschaftsinformatik* **2021**, *58*, 565–579. [CrossRef]
7. Beinke, J.H.; Fitte, C.; Teuteberg, F. Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study. *J. Med. Internet Res.* **2019**, *21*, e13585. [CrossRef] [PubMed]
8. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2009. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 5 April 2024).
9. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain Meets Cloud Computing: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]
10. Erler, C.; Schinle, M.; Dietrich, M.; Stork, W. Decision model to design a blockchain-based system for storing sensitive health data. In Proceedings of the European Conference on Information Systems, Timișoara, Romania, 18–24 June 2022.
11. Xu, X.; Bandara, H.D.; Lu, Q.; Weber, I.; Bass, L.; Zhu, L. A Decision Model for Choosing Patterns in Blockchain-Based Applications. In Proceedings of the 2021 IEEE 18th International Conference on Software Architecture (ICSA), Stuttgart, Germany, 22–26 March 2021.
12. Erler, C.; Hu, S.; Danelski, A.; Stork, W.; Sunyaev, A.; Gersch, M. Threat Modeling to Design a Decentralized Health Data Management Application. In *Information Technology and Systems*; Springer: Cusco, Peru, 2023.
13. Shostack, A. *Threat Modeling*; Wiley: Hoboken, NJ, USA, 2014.
14. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77. [CrossRef]

15. Nickerson, R.C.; Varshney, U.; Muntermann, J. A method for taxonomy development and its application in information systems. *Eur. J. Inf. Syst.* **2013**, *22*, 336–359. [[CrossRef](#)]
16. Shevchenko, N.; Chick, T.A.; O’Riordan, P.; Scanlon, T.P.; Woody, C. Threat Modeling: A Summary of Available Methods. Software Engineering Institute, Carnegie Mellon University. August 2018. Available online: <https://insights.sei.cmu.edu/library/threat-modeling-a-summary-of-available-methods/> (accessed on 5 April 2024).
17. Wüst, K.; Gervais, A. Do you Need a Blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.
18. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-Based Data Preservation System for Medical Data. *J. Med. Syst.* **2018**, *42*, 141. [[CrossRef](#)]
19. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140. [[CrossRef](#)] [[PubMed](#)]
20. Hawig, D.; Zhou, C.; Fuhrhop, S.; Fialho, A.S.; Ramachandran, N. Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation-Compliant Health Data Exchange: A Use Case in Blood Glucose Data. *J. Med. Internet Res.* **2019**, *21*, e13665. [[CrossRef](#)]
21. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
22. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
23. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [[CrossRef](#)] [[PubMed](#)]
24. Xiao, Z.; Li, Z.; Liu, Y.; Feng, L.; Zhang, W.; Lertwuthikarn, T.; Mong Goh, R.S. EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 998–1003.
25. Chang, E.Y.; Liao, S.-W.; Liu, C.-T.; Lin, W.-C.; Liao, P.-W.; Fu, W.-K.; Mei, C.-H.; Chang, E.J. DeepLinQ: Distributed Multi-Layer Ledgers for Privacy-Preserving Data Sharing. In Proceedings of the 2018 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), Taichung, Taiwan, 10–12 December 2018; pp. 173–178.
26. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain *IEEE Access* **2019**, *7*, 136704–136719. [[CrossRef](#)]
27. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [[CrossRef](#)]
28. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access* **2019**, *7*, 66792–66806. [[CrossRef](#)]
29. Hanley, M.; Tewari, H. Managing Lifetime Healthcare Data on the Blockchain. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCOM/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 246–251.
30. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. *IEEE Access* **2019**, *7*, 164595–164613. [[CrossRef](#)]
31. Thwin, T.T.; Vasupongayya, S. Blockchain Based Secret-Data Sharing Model for Personal Health Record System. In Proceedings of the 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA), Krabi, Thailand, 14–17 August 2018; pp. 196–201.
32. Theodouli, A.; Arakliotis, S.; Moschou, K.; Votis, K.; Tzovaras, D. On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1374–1379.
33. Zaghoul, E.; Li, T.; Ren, J. Security and Privacy of Electronic Health Records: Decentralized and Hierarchical Data Sharing using Smart Contracts. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 375–379.
34. Zheng, X.; Mukkamala, R.R.; Vatrappu, R.; Ordieres-Mere, J. Blockchain-based Personal Health Data Sharing System Using Cloud Storage. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018; pp. 1–6.
35. Zhou, T.; Li, X.; Zhao, H. Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique Monitoring and Scientific Exercise Guiding. *J. Med. Syst.* **2019**, *43*, 305. [[CrossRef](#)] [[PubMed](#)]
36. Lee, Y.L.; Lee, H.A.; Hsu, C.Y.; Kung, H.H.; Chiu, H.W. SEMRES—A Triple Security Protected Blockchain Based Medical Record Exchange Structure. *Comput. Methods Programs Biomed.* **2022**, *215*, 106595. [[CrossRef](#)]

37. Zhang, L.; Zhang, T.; Wu, Q.; Mu, Y.; Rezaeibagha, F. Secure Decentralized Attribute-Based Sharing of Personal Health Records With Blockchain. *IEEE Internet Things J.* **2022**, *9*, 12482–12496. [CrossRef]
38. Cao, Y.; Sun, Y.; Min, J. Hybrid blockchain-based privacy-preserving electronic medical records sharing scheme across medical information control system. *Meas. Control* **2021**, *54*, 1286–1299. [CrossRef]
39. Hu, C.; Li, C.; Zhang, G.; Lei, Z.; Shah, M.; Zhang, Y.; Xing, C.; Jiang, J.; Bao, R. CrowdMed-II: A blockchain-based framework for efficient consent management in health data sharing. *World Wide Web* **2022**, *25*, 1489–1515. [CrossRef] [PubMed]
40. Wang, Y.; He, M. CPDS: A cross-blockchain based privacy-preserving data sharing for electronic health records. In Proceedings of the 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), Chengdu, China, 24–26 April 2021; pp. 90–99.
41. Jayasinghe, J.G.L.A.; Shiranthaka, K.G.S.; Kavith, T.; Jayasinghe, M.H.D.V.; Abeywardena, K.Y.; Yapa, K. Blockchain-based secure environment for electronic health records. In Proceedings of the 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 3–5 October 2022.
42. Lee, S.; Kim, J.; Kwon, Y.; Kim, T.; Cho, S. Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study. *J. Med. Internet Res.* **2022**, *24*, e29108. [CrossRef] [PubMed]
43. Zou, R.; Lv, X.; Zhao, J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Inf. Process. Manag.* **2021**, *58*, 102604. [CrossRef]
44. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. A cooperative architecture of data offloading and sharing for smart healthcare with blockchain. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021.
45. Boumezebur, I.; Zarour, K. Blockchain-Based Electronic Health Records Sharing Scheme with Data Privacy Verifiable. *Appl. Med. Inform.* **2021**, *43*, 124–135.
46. Gupta, A.; Rodrigues, R.; Tripathi, A.; Coutinho, R.; Gomes, J. Blockchain for EHR: An off-chain based approach. In Proceedings of the 2022 IEEE Region 10 Symposium (TENSYP), Mumbai, India, 1–3 July 2022.
47. Lin, G.; Wang, H.; Wan, J.; Zhang, L.; Huang, J. A blockchain-based fine-grained data sharing scheme for e-healthcare system. *J. Syst. Arch.* **2022**, *132*, 102731. [CrossRef]
48. Zaghoul, E.; Li, T.; Mutka, M.W.; Ren, J. d-MABE: Distributed Multilevel Attribute-Based EMR Management and Applications. *IEEE Trans. Serv. Comput.* **2022**, *15*, 1592–1605. [CrossRef]
49. Sabu, S.; Ramalingam, H.M.; Vishaka, M.; Swapna, H.R.; Hegde, S. Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain. *Glob. Trans. Proc.* **2021**, *2*, 429–433. [CrossRef]
50. Lee, H.A.; Kung, H.H.; Udayasankaran, J.G.; Kijisanayotin, B.; Marcelo, A.B.; Chao, L.R.; Hsu, C.Y. An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study. *J. Med. Internet Res.* **2020**, *22*, e16748. [CrossRef]
51. Huang, H.; Zhu, P.; Xiao, F.; Sun, X.; Huang, Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Comput. Secur.* **2020**, *99*, 102010. [CrossRef]
52. Zhao, F.; Yu, J.; Yan, B. Towards cross-chain access control model for medical data sharing. *Procedia Comput. Sci.* **2022**, *202*, 330–335. [CrossRef]
53. Li, L.; Yue, Z.; Wu, G. Electronic medical record sharing system based on hyperledger fabric and InterPlanetary file system. In Proceedings of the 2021 5th International Conference on Compute and Data Analysis, Sanya, China, 2–4 February 2021.
54. Ramesh, D.; Mishra, R.; Atrey, P.K.; Edla, D.R.; Misra, S.; Qi, L. Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage. *Alex. Eng. J.* **2023**, *68*, 205–226. [CrossRef]
55. Qin, Q.; Jin, B.; Liu, Y. A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain. *BioMed Res. Int.* **2021**, *2021*, 6676171. [CrossRef] [PubMed]
56. Baldin, I.; Chase, J.; Crabtree, J.; Nechyba, T.; Christopherson, L.; Stealey, M.; Kneifel, C.; Orlikowski, V.; Carter, R.; Scott, E.; et al. ImPACT: A networked service architecture for safe sharing of restricted data. *Future Gener. Comput. Syst.* **2022**, *129*, 269–285. [CrossRef]
57. Lomotey, R.K.; Kumi, S.; Deters, R. Data Trusts as a Service: Providing a platform for multi-party data sharing. *Int. J. Inf. Manag. Data Insights* **2022**, *2*, 100075. [CrossRef]
58. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. *Sensors* **2020**, *20*, 483. [CrossRef]
59. Registering and Enrolling Identities with a CA. Available online: https://hyperledger-fabric-ca.readthedocs.io/en/latest/deployguide/use_CA.html (accessed on 24 October 2023).
60. Rawal, B.S.; Manogaran, G.; Peter, A. *Cybersecurity and Identity Access Management*; Springer: Singapore, 2023.
61. Al-Hamdani, W.A. Cryptography Based Access Control in Healthcare Web Systems. In Proceedings of the InfoSecCD'10: 2010 Information Security Curriculum Development Conference, Kennesaw, GA, USA, 1–3 October 2010; pp. 66–79.

62. PasswordBits. The Difference between Password vs. Encryption Protection. Available online: <https://passwordbits.com/the-difference-between-password-vs-encryption-protection/> (accessed on 29 December 2023).
63. Schinle, M.; Erler, C.; Stork, W. Data Sovereignty in Data Donation Cycles—Requirements and Enabling Technologies for the Data-driven Development of Health Applications. In Proceedings of the 54th Hawaii International Conference on System Sciences, Maui, HI, USA, 5–8 January 2021; pp. 3972–3981.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.