electronics

Article

Blockchain-Based Access Control in a Globalized Healthcare Provisioning Ecosystem

Stavros Salonikias [1], Marie Khair [2], Theodoros Mastoras [1] and Ioannis Mavridis [1,*]

[1] Department of Applied Informatics, University of Macedonia, 546 36 Thessaloniki, Greece
[2] Department of Computer Science, Faculty of Natural and Applied Sciences, Notre Dame University, Zouk Mosbeh P.O. Box 72, Lebanon
* Correspondence: mavridis@uom.edu.gr; Tel.: +30-231-089-1868

Abstract: The COVID-19 pandemic further outlined the importance of global healthcare services provisioning for diagnosing and treating patients who tend to travel and live for large periods away from home and can be anywhere at any given time. Advances in technology enable healthcare practitioners to access critical data regarding a person's health status to provide better services. Medical data are sensitive in nature, and therefore, a reliable mechanism should ensure that only authorized entities can access data when needed. This paper, through a layered consideration of a Globalized Healthcare Provisioning Ecosystem (GHPE), reveals the interdependencies among its major components and suggests a necessary abstraction to identify requirements for the design of an access control suitable for the ecosystem. These requirements are imposed by the nature of the medical data as well as by the newly introduced potentials of Internet of Medical Things (IoMT) devices. As a result, an attribute-based access control framework is proposed aiming to provide prompt and secure access to medical data globally by utilizing state-of-the-art technologies and standards, including Next-Generation Access Control (NGAC), blockchain and smart contracts. Three types of smart contracts are proposed that enable access control to implement attribute and policy stores where policy classes and attributes are decentralized and immutable. In addition, the usage of blockchain-based distributed identities allows patients to be in control of access to their medical data and also enables healthcare service providers to access medical data promptly and reliably through the proposed access control framework. The qualitative characteristics of the proposed approach toward a decentralized and patient-centric access control in GHPE are demonstrated and discussed based on an application paradigm.

Keywords: access control; NGAC; blockchain; Ethereum; smart contracts; healthcare; IoMT

check for updates

Citation: Salonikias, S.; Khair, M.; Mastoras, T.; Mavridis, I. Blockchain-Based Access Control in a Globalized Healthcare Provisioning Ecosystem. *Electronics* **2022**, *11*, 2652. https://doi.org/10.3390/electronics11172652

Academic Editor: Gemma Piella

Received: 18 June 2022
Accepted: 20 August 2022
Published: 25 August 2022

1. Introduction

A healthcare system, as defined by the World Health Organization, consists of all organizations, people, and actions whose primary intent is to promote, restore or maintain health. Telemedicine, health monitoring, and assisted living are some examples enabled by the blending of Information and Communication Technologies (ICT) into the provision of health services. Healthcare provisioning was once taking place only in specialized facilities, such as hospitals or medical centers. Advances in communication technology though are the solid enabler toward transforming healthcare into an ongoing process, while the patient is at home or even traveling or performing any activity indoors or outdoors. [1]. Medical devices represent one of the fastest-growing sectors of the IoT market. It is expected that the IoT in the healthcare and lifestyle market will reach around USD 1824 billion by 2026 and up to USD 3400 billion by 2030 [2]. Additionally, the Internet of Medical Things (IoMT) realizes the use of IoT in healthcare provisioning to produce a better outcome for patients [3].

New technologies enable people to access health services and medical data in everyday life and provide several advantages ranging from specific illness follow-up and treatment (such as cancer, diabetes, etc.) [4–6], to tracking patients and staff, to improving the patients' care inside and outside hospitals, to collecting, to reporting, and analyzing real-time data. Moreover, IoMT and other still emerging technologies, such as 6G [7] and Smart Radio Environments [8], can enable the deployment of patient-centric and context-aware collaborative medical systems in various environments ranging from hospital floors, operating rooms, and intensive care units to public service and health provider premises [9], realizing the vision for continuous healthcare provisioning and assisted living. All these technologies can also be utilized to support the use of better diagnostic tools, advanced and timely treatment for patients, and significant improvement of the life quality for human beings [10]. Access to this kind of sensitive data though is restricted under regulatory and legal controls, such as the GDPR in EU [11], so that no entity should be able to perform any operation without the former approval of the medical data owner, i.e., the patient.

People nowadays tend to move a lot inside or outside a state or country. However, the COVID-19 pandemics outlined the need for health services and medical data to be available anytime, anywhere, beyond the logical or physical borders of an organization or a country and in cooperation among different healthcare providers. In most cases today, there are already discrete and, on many occasions, heterogeneous ICT platforms in place, which are used by those providers to exchange data with each other. However, there are still cases where medical data are stored within medical provider premises, offline, and when needed by another medical provider, the patient (or an authorized proxy) may need to obtain a copy of the records himself. Hence, this lack of automation can lead to the same set of information being stored in different places, owned by different stakeholders, and moreover, induce delays that may have a negative impact on the patient's health. To address those considerations, the EU is currently working on electronic cross-border health services and a European health data space ecosystem [12].

The heavy digitization and strict regulation [13], though, urge the need to not only manage the storage, distribution, and availability of the information but also the ability to enforce safeguards on accessing medical data. Access control solutions are thus used for limiting actions or operations that an authenticated and authorized subject can perform on an object. In legacy systems, the subject is usually a user or a process acting on behalf. Usually, the subject presents a specific identity that should be verified during the authentication process. Thus, strong authentication is a prerequisite for a successful authorization process [14]. However, in the versatile ecosystem under consideration in the present work, many actors tend to be completely unknown before the authorization process. During the study presented in the following of this paper, the following research questions need to be answered:

- How can a global healthcare ecosystem could be considered and analyzed?
- What are its specific access control challenges and requirements?
- What technologies and standards should be utilized in addressing those requirements?
- How should the selected technologies and standards be deployed and orchestrated to accommodate the access control system components?

The main contribution of this paper is to propose an access control framework that addresses the particular requirements of the GHPE by combining a set of widely accepted state-of-the-art technologies and standards, including the blockchain, smart contracts, distributed identities, and NGAC. Specifically, we provide a layered consideration of the GHPE and examine the derived access control requirements based on its particular aspects. We then propose an access control framework, suitable for the GHPE, based on NGAC [15] to allow flexible policy management and access enforcement, as well as the deployment perspective over a public blockchain infrastructure, such as Ethereum. The use of the blockchain infrastructure in this work is twofold. On the one hand, it is used to provide an immutable store for distributed identities, policies, attributes, and audit logs; meanwhile, on the other hand, the selection of Ethereum allows for the use of smart contracts to accommodate NGAC components and to provide the required flexibility, transparency and trustworthiness. To our knowledge, there are no other works in the literature presenting such a holistic approach that enables borderless and secure access to medical data throughout the globe, without the intervention of a central authority or registrar.

Firstly, in Section 2, we provide background information on the GHPE components, as well as the technologies and standards used in this paper. Section 3 presents relative work on access control for similar environments, while in Section 4, we define a set of access control requirements in the GHPE. Then, Section 5 describes a layered consideration of the GHPE that provides the foundation on which the proposed access control framework is built and presented in Section 6. An application paradigm is presented in Section 7 to outline the overall functionality of the proposed system, and a discussion on the qualitative characteristics of the proposed approach is provided in Section 8, Finally, Section 9 concludes the paper.

2. Background

For developing an access control system suitable for the GHPE, a set of contemporary technologies and standards will be utilized and blended to provide a novel steppingstone toward a patient-centric access control that includes authentication, authorization, and accounting.

2.1. GHPE Components

In their work, Heart et al. [16] distinguish between various patient-related health information which consists of Electronic Medical Records (EMR), Patient Health Records (PHR), and Electronic Health Records (EHR). The difference across those three categories relies on the nature and purpose of the included medical data, storage location, and the management entity. Specifically, EMR are usually produced when patients visit medical facilities to undergo medical operations and are stored either on-premises or in a private or public cloud owned by the medical provider. Accordingly, access to those records is managed by the provider itself. PHR are data created by the patient or by devices one owns and could also be handled by the patients themselves. Hence, among PHR, one may find records regarding health status (such as heart rate, blood pressure, etc.) as well as some portions of medical history (allergy information, vaccination history, etc.). Finally, EHR are those patient-related medical records that are shared among providers, either exchanged via direct communication lines or by being uploaded and handled by an intermediate trusted entity, such as a ministry or any other trusted organization. For simplicity, the term EHR will be used throughout this paper to refer to any type of medical record.

While EHR could be stored in the cloud utilizing distributed filesystems, the fact that medical devices need to be in close vicinity to patients and are sometimes low in resources makes cloud storage quite challenging. Moreover, the heterogeneity in regulations across countries and the sensitive nature of medical data would also make it difficult to propose a common storage space with data navigating across regions. Taking these under consideration, we promote the resting of data to medical provider premises or private cloud storage, retaining the current storage schema. Having individual providers store medical information themselves instead of using a potential common distributed store also helps in being conformant to requirements imposed by regulations (such as GDPR in the EU) and moreover can be more easily adopted to current practice. There are also medical devices used that are usually deployed in close vicinity of the patient and are accessed via respective Virtual Objects (VO) which are deployed in the fog, mist, or edge layer [17], depending on the operational requirements of the devices themselves or the personal network.

In GHPE, we distinguish between two groups of stakeholders: the healthcare service providers and the healthcare service provision receivers. Providers are defined as any entity participating in the provision of healthcare services. Examples of such stakeholders are actors on behalf of hospitals, diagnostic centers, insurance companies, and even research facilities. In an Access Control System (ACS), the stakeholders that request access to resources, either EHR or medical devices, are named “users” in accordance with the NIST NGAC convention [15]. On the other hand, healthcare receivers are the patients including any person that owns EHR and medical devices and undergoes medical operations. Patients, as data owners, should be able to perform administrative operations, thus setting access control policies to define who and under which situations individuals will be able to gain access to those resources.

We also define a Healthcare Provisioning Unit (HPU) as any autonomous healthcare provisioning environment which can be a whole clinic, a hospital department, a personal network, an ambulance, etc. To provide holistic health services, groups of HPUs can form domains that interoperate on common tasks, hence forming a collaborative system as described by [18] and providing consistent access control services. An example of a domain can be a set of HPUs of a state or a country. Finally, further cooperation among domains can lead to even larger entities, such as federations of domains. A federation can be an inter-state health provisioning system, including, for example, European medical providers toward implementing the European healthcare card.

2.2. Authentication Technologies

Authentication has always been essential to access control, being the process via which a system gains confidence in the presented identity of a communication partner [19] and distinguishes between the specific entity and any other entity within the GHPE. Upon an access request, the user needs initially to identify oneself, and then, the deployed ACS evaluates his requests against defined policies to decide whether the requestor has enough rights to access resources or not. Therefore, the requestor should present some “claim” to prove oneself and the validity of his request. This claim, which the requestor controls, is used to prove his identity, and it is also used through valid attestations from concerned parties in evaluating the right to the services he is requesting access to [20].

In classical systems, the use of identifiers was managed by centralized providers. However, this mechanism suffers from several vulnerabilities such as single point of failure, loss of privacy, and lack of interoperability, which are unacceptable in the GHPE. Therefore, the need for decentralized identifiers and verifiable claims implemented on blockchain [21] encounters the above weaknesses. Mühle et al. in their work [13] present the Self-Sovereign Identities (SSI) as an identity management system to help identity owners maintain their identities. SSI is user-centric and allows the user to maintain the same identity throughout the GHPE, deprecating the need for centralized identity providers. Verifiable Credentials (VC) include a set of claims and are bound to Decentralized Identifiers (DID) that are globally unique references to DID documents [22]. Identifiers refer to entities that can be a person or an IoT device, while VC are digital attestations of the identity holder. The issuance and verification of VC require several roles: the entity holding the credential, the issuer, and the verifier. The deployment of DID requires cooperation among several entities, namely issuers, who can be governmental bodies or hospitals and are responsible for the issuance and revocation of claims. Requestors are either: patients, healthcare service providers, or insurers. Once an entity obtains one or more claims, it can request verification through public key cryptography and can therefore proceed.

The claims that a requestor should present form a part of VC that comprises three main parts [23]:

- The credential metadata, which includes an ID, the type, the issuer, the issuance date, and the credential subjects.
- The claim, which contains the attributes the subject wants to be able to show to the receivers. Only the attributes which the requestor chooses to include can be accessed by the verifier. Any attribute that the requestor chooses not to include will be kept secret.
- The proof, which specifies the signature type used to validate the claim (which uses asymmetric encryption), the date created, the verification methods, and others.

A DID is used by the verifier to prove the authenticity of the claim. This authenticity is performed using the private key of the issuer and verified using his corresponding public key. To be able to become a member of the ecosystem, as either patient or user, every individual should first create a DID and then contact a Claim Issuer to receive VC. Claim Issuers can be deployed and maintained by public authorities or any other credible organization. Patients and users can present their DID whenever a new access request is made. A relative approach, using a centralized ACS, has been proposed by Belchior et al. [24]. Usually, a patient does not need to hold multiple identities, which is the case for users that may provide a different identity depending on access context, i.e., the specific role one has in the healthcare provisioning process.

2.3. Authorization Technologies

The need for prompt, global services, especially in the pandemic era, urges the need for timeless access to patient EHR, to give medical practitioners a better understanding of patients' conditions so that they can proceed with the appropriate treatment. On the other hand, a solid ACS is called to ensure that no unauthorized access to sensitive data may occur. In this environment, though, some basic principles apply. Firstly, data are owned by the patient who is responsible for creating rules that define when, where and to whom access to his EHR and his own medical devices is allowed. Secondly, all entities responsible for providing healthcare services should be able to request access and, depending on the access decision, access will either be permitted or not. By producers, we refer to medical providers who produce medical data or provide medical devices. By consumers, we refer to medical providers who need access to data or devices to provide medical assistance or insurance services.

In past decades, various access control approaches have been proposed, among which those that have received the most recognition were: Mandatory Access Control, Discretionary Access Control, and Role-Based Access Control [25–27]. However, these approaches fail to adapt to the access control requirements in GHPE as described in the next Section 3, which is populated by heterogeneous devices and is operating in a versatile environment. Access control decision making in GHPE needs to consider contextual information [28] related to subjects, objects, and the environment in which access control entities reside or operate. In recent years, Attribute-Based Access Control (ABAC) has prevailed as a contemporary access control approach. The key differentiator in ABAC compared to other approaches is the use of attributes [29]. An attribute is expressed as a label-value tuple, and it can be used to characterize the subject, the object, and the environment. Accordingly, policies and decisions are based on attribute values (instead of identities only) at a given time. Therefore, ABAC can support context-aware policies. Nevertheless, although for standalone systems, the attribute definition does not seem to be a problem, and in the case of multi-domain federations, it may be confusing in a twofold way. Firstly, the label of an attribute may be defined differently in each HPU or domain and secondly, the possible values may be expressed on different scales. Hence, there is a need for a standardized definition of attributes.

The various kinds of points in NGAC are referred in the next section of this paper as NGAC components.

2.4. NGAC Standards

As for the authorization of authenticated entities, NGAC, proposed by NIST [15], is a promising set of standards to deploy access control in distributed environments. NGAC supports the development of ACS with modular architecture. According to NGAC, an access request submitted by a subject, which could be identified through SSI, is intercepted by the Policy Enforcement Point (PEP) which then sends it to the Policy Decision Point (PDP). PDP evaluates the request considering policies defined in the Policy Administration Point (PAP) and attributes from the Policy Information Point (PIP) to reach a decision. The decision is then sent back to PEP which issues an appropriate command to the specific

Resource Access Point (RAP) to execute the operation and return status and any additional information derived from the execution. PEP also submits the context of access enforcement to the Event Processing Point (EPP) to deal with administrative operations, which are expressed in terms of obligations.

PEPs are usually located in close vicinity to edge devices or datastores. In most of the IoMT cases though, edge devices lack the resources to enforce decisions. Therefore, there is an implementation of RAPs, which can be supported by VOs [30]. VOs provide the necessary abstractions for the ACS to function as intended, uncoupled from hardware limitations, considering any kind of object likewise. Additionally, using a VO that represents a physical one throughout its lifecycle leaves the burden of having to consider where the physical object is connected and is available at any given time. To apply ABAC throughout the GHPE, an identity store, a policy store, and an attribute store should exist.

2.5. Ethereum

Due to its unique characteristics [31], blockchain can provide the ideal platform for a decentralized and tamperproof ledger of identities, policies, and attributes. Ethereum implements blockchain, which can be thought of as a decentralized database that stores transactions and implements smart contracts [32]. A transaction is a transfer of values between different entities that are signed, broadcasted, and finally collected in blocks. A smart contract is an autonomous script stored on the blockchain with a unique address. Smart contracts can be created by any user and posted as transactions in Ethereum to carry different structures such as program execution, storage, or even an account balance. The smart contract's code is executed whenever it is called by a user or from another smart contract. Each interaction with the contract is stored as a transaction in the blockchain. These characteristics make blockchain capable of providing immutability, transparency, and auditability. In addition, logging that is kept on the blockchain ensures accountability due to the tamperproof infrastructure and high availability which are guaranteed by the blockchain infrastructure. Thus, it is proposed by several researchers [33,34] as a solution for healthcare sector environments due to its ability to provide a peer-to-peer network, where participants can interact with each other in a verifiable and secure manner, without a trusted intermediary party, based on a consensus mechanism between nodes.

In the GHPE, Ethereum is proposed to be used to accommodate the NGAC components providing a global decentralized deployment platform. However, context plays a significant role in access decisions, and contextual attributes are usually located outside the blockchain. As a solution, Oracles can allow Ethereum, and specifically smart contracts, to interact with the real world [35].

3. Related Work

In recent years, the use of blockchain in access control has gained significant interest due to the unique characteristics it provides. Ouaddah et al. [36] propose an access control framework to satisfy IoT security and privacy needs based on blockchain. The authors introduce new types of transactions such as grant, get, delegate, and revoke, and it is the user who has full access control over the data that are implemented through smart contracts. Satamraju [37] proposes a framework that integrates IoT with blockchain. This model proposes the usage of smart contracts to handle authentication, authorization, and access control. The framework proposes three layers, namely: storage, business, and application layers. Ali et al. in [38] propose to use multiple certificate authorities within cross-domain or cross-organizations implemented for a flexible access control over data within a Hyperledger fabric. Moreover, Kumar and Tripathi in [39] proposed an access control policy that has four types of rules defined for read, remark, update and delete. The rules are defined using smart contracts and implemented on a Hyperledger composer modeling tool that provides dynamic access control functionality on the blockchain. The model was implemented using an enhanced Bell–Lapadula model where each peer is associated a clearance level.

In the healthcare sector, there is also ongoing research activity with several works utilizing blockchain such as Albreiki et al. [40], who proposed a decentralized access control for the IoT data that are implemented through smart contracts on an Ethereum blockchain. Data are stored on several storage services such as the cloud, and oracles are used to interact between the blockchain and the external data. Hossein et al. [41] propose the usage of two blockchains: one for storing the patients' healthcare data and another for storing the access control policies. The proposed model allows data owners to define the access policies on their sensitive data that are stored on an edge device instead of being stored on the cloud. In addition, it uses hierarchical clustering to improve scalability and throughput. Dubovitskaya et al. propose in [42] a patient-centric system to allow the patients to manage their EHRs. They use a permissioned blockchain system where they too use on-chain for management metadata, and off-chain will be used to store the encrypted EHR. Mubarakli et al. in [43] use a permissioned blockchain to implement a privacy-preserving access control between the different users who can be patients, doctors, service providers and institutions. Data within the system are encrypted using symmetric keys, and all users have public and private keys. It is the patient who decides about the access control privileges. Alsayegh et al. in [44] use proxy re-encryption of the EHR using the patient's public key to provide a fine-grained access control. In addition, they use two types of blockchain: a private blockchain used to store the encrypted EHR and a consortium blockchain to store an encrypted index in the smart contract.

One important aspect that is also under consideration is the storage of medical data in a common space. Younis et al. in [45] propose to use blockchain mainly through the implementation of smart contracts to keep track of the access control rules that are needed to regulate access between healthcare providers patients and the cloud. Storing data on the cloud guarantees privacy regulations using encryption. In addition, a new data-driven authentication method is used that changes the key per packet, which makes the system robust against cryptanalysis attacks. Jayabalan and Jeyanthi [46] propose the usage of IPFS for the storage of the encrypted electronic health records, and only pointers to the specific records are stored within the blockchain. Two-factor authentication and multi-factor authentication are proposed to give better security in addition for the patients to be in control of access to their data. Cong et al. [47] propose the combination of the blockchain, IPFS, and cipher text policy attribute encryption to supply privacy-preserving IoT data. The proposal categorizes users into two groups: user owners and users requestors. User owners can decide on the access policy and encrypt the data stored using CP-ABE in the IPFS, while the hash of the data and the metadata are stored on the blockchain. Meanwhile, user requestors search for the metadata in the blockchain and can retrieve the ciphertext in the IPFS only if their attributes validate the specified condition in the policy. Azbeg et al. [48] propose the usage of blockchain in addition to IPFS to secure the access to the IoT healthcare devices. The system encapsulates three actors: patients, physicians, and hospitals that are connected through the blockchain. Health data are collected by the patients, stored on IPFS and a hash of the data is stored on the blockchain. Proxy re-encryption is used to store the data and preserve its security.

Smart contracts are also being considered. Geetha and Balakirshnan [49] propose the usage of several smart contracts for user authentication in IoT. These contracts implemented on Ethereum blockchain communicate with local gateways to the IoT devices and provide distributed and decentralized access control maintaining scalability and security.

After the study of related works, and having identified the need for global healthcare provisioning, we propose a holistic approach in the GHPE that uses already established state-of-the-art technologies and standards and can be adapted in current healthcare practice without having to relocate data or disrupt healthcare practice.

4. Access Control Challenges and Requirements in GHPE

When providing healthcare services to patients, a set of EHR can be valuable for medical practitioners. The difference in record types though does not solely rely on the location type and location infrastructure which is owned by the providers themselves. The format of the data itself also varies significantly, while different record categories may produce unique or proprietary formats. For example, radiology departments usually store images using Picture Archiving and Communication Systems (PACS) servers, whereas laboratories can use Laboratory Information Systems to store analysis results. Furthermore, a gigantic set of data can be produced by patients' personal devices and then stored in various locations. As a result, different storage locations and heterogeneous data ownership impose significant obstacles to data diffusion and access, especially when another user or any other authority may need prompt access to it.

In legacy healthcare systems, patients and users are identified in the realm of each healthcare provider, which means that there exist different identity stores where users should have been registered. Information of any identity is provided and maintained by centralized, private, or public identity providers, to which the patient should have been registered. To use those entities globally, they should have been registered in centralized authorities and accessible from all healthcare provisioning organizations. This, apart from performance issues, would also impose security concerns such as authorities being single-point-of-failure, managed and maintained by entities that need to be trusted by all participants, and, moreover, possible regulatory inconsistencies among countries where providers reside. To remediate such issues, a decentralized system that can ensure that identities are globally unique and verifiable will be of great benefit.

An ACS suitable for healthcare, to its full extent, should be able to accommodate legacy ICT as well as novel IoMT and other medical applications. One should not disregard that a patient can be anywhere in the world and consume medical services from different providers anytime. Moreover, an ACS should be able to function in a multi-domain ecosystem where subjects and objects such as patients, users, and resources, respectively, might pre-exist and roam or be seen for the first time. Data should always be owned by the patient who, depending on the situation, must be able to control and administer access to her data throughout the GHPE.

The COVID-19 pandemic has outlined the importance of global medical data access and availability for either healthcare provisioning or for health status validation (e.g., vaccination certificates) by authorized entities. Nevertheless, the highly sensitive nature of medical information dictates the need for an access control mechanism that can ensure privacy by permitting access to data only to authorized entities in accordance with the principles of least privilege, separation of duties, and data abstraction as well as the ability of the patient to be the actual data owner as well as the one who controls who has access to it.

Healthcare services are heavily reliant on the context. The term context is defined as "any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." [50]. For example, the context regarding a patient being in the Intensive Care Unit (ICU) is different from the context where the same patient undergoes some routine examination by a physician or is at home being monitored by some sensors.

Although there are studies on defining access control requirements for medical information [51–53], the diverse nature and the need for global access are not usually taken under consideration. Moreover, contemporary medical services do heavily rely on IoMT, which includes embedded and pervasive devices able to collect valuable health information or perform medical actions (e.g., induce a medicine). These devices can be integrated into the healthcare practice and cannot be separated from it [54]. Hence, all challenges of ubiquitous and pervasive systems are also applied in the IoMT. Moreover, also taking IoMT under consideration, an access control system should also fulfill the requirements of resource-constrained environments and still be usable and able to scale. The criticality of its use mandates that resiliency and interoperability are also ensured.

Table 1 depicts a basic set of challenges that an access control system should be able to address toward defining an ACS suitable for the GHPE.

Table 1. Access control challenges.

Challenge	Description
Availability	Services should be always available
Mobility	People nowadays travel a lot, and access to medical information should be provided to a large extent, even globally.
Identification	Entities must be able to be identified and authenticated.
Heterogeneity	Systems and technologies used are heterogeneous and may use proprietary technologies or data formats.
Storage efficiency	Sufficient storage space should be provided, and data should be globally accessible.
Data deduplication	A unique data record should exist to avoid discrepancies or misuse of storage.
Information ownership	Information should be owned by the patients themselves.
Context awareness	Context parameters should be considered.
Privacy	Privacy borders should not be crossed. Marx [16] defines it in terms of privacy violation, thus as the crossing of natural, social, spatial, and transitory borders. In this context, any solution should apply all necessary safeguards to ensure that there is no possible means of compromising, directly or indirectly, any of those barriers.
Decentralization	In collaborative environments, objects should be shared among stakeholders on the same or different domains. Moreover, when multiple domains, including several HPUs, form federations, the problem becomes more intense [8]. In a collaborative system of such extent, any trusted authority acting as a central identity provider may turn into a single point of compromise or failure. To mitigate this threat, decentralization should be considered.
Orchestration	Conflicting policies between domains should be avoided or resolved prior to any access control decisions.
Interoperability	Discrete systems should be able to exchange information.
Standardization	The same set of standards should apply throughout the domain for the solution to be applied globally.
Resilience	The whole system should be resilient to failures that may be caused by accidental or targeted attacks.
Scalability	The system should be able to adapt while stakeholder and resource numbers increase.
Usability	Policy administration controls should be usable for non-technical users [4].
Efficiency	Adapt and function in a resource-constrained environment with acceptable performance.
Accountability	Accounting, also known as auditing, is the process of retaining information regarding actions performed in a system and is used to detect violations or security flaws. An ACS is not considered a complete solution unless auditing is applied [55]

5. Layered View of the GHPE

Out of the plenty of technologies involved beyond legacy ICT systems, the most prevalent one is Wireless Sensor Networks, which provides the platform for sensors that are attached or placed in close vicinity to the patients, to monitor a large set of health and environmental parameters. These devices along with medical Cyber-Physical Systems, embedded computers, and mobile devices are located near, or are worn by the patient, and they are architecturally connected to the edge of the network.

However, many of the devices in this area lack the power and computing resources to store and process all collected information, which can be massive. To solve this issue, a platform that scales in both storage and processing efficiency is required. The cloud has provided a resourceful platform that can be used to store and process data by exporting relative services to consumers who can post, process, and obtain results. These services, namely Cloud-Based Services (CBS), encapsulate various cloud service models to provide greater benefit and dynamicity to the users, such as Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a Service (SaaS), and Database as a Service (DaaS).

CBS offers improved performance and storage processing. Cloud-based IoMT, though, may impose some weaknesses in terms of connection characteristics, which may be alleviated by having the services much closer to the requesters and, therefore, provide much better connection characteristics. The need to improve those characteristics, such as latency and jitter, gave birth to the concept of the fog [10]. The fog utilizes a set of servers and other nodes, physical or virtual, to bring cloud services closer to data producers and consumers in the edge, and it provides significant advantages, especially in resource-intensive environments such as IoMT. Fog computing may offer, among others, low latency (due to more physical proximity), lesser bandwidth problems (due to distribution and aggregation) and more consistency and power efficiency. Moreover, bringing cloud services near the edge enables services to be context-aware and manage takeover load from both the cloud and the edge resources.

In the case of IoMT though, many low-powered heterogeneous devices are in operation. These devices may consume hard-to-find power when communicating [56] or use proprietary communication protocols. To accommodate communication between edge devices and the fog, a discussion on a new layer, namely the mist, blended into the fog and attached close to the edge has emerged [57,58]. Mist is accommodated into the network fabric itself and coordinates data transmissions between devices at the edge and fog nodes.

Figure 1 represents a layered view of several technologies exploited by the GHPE.

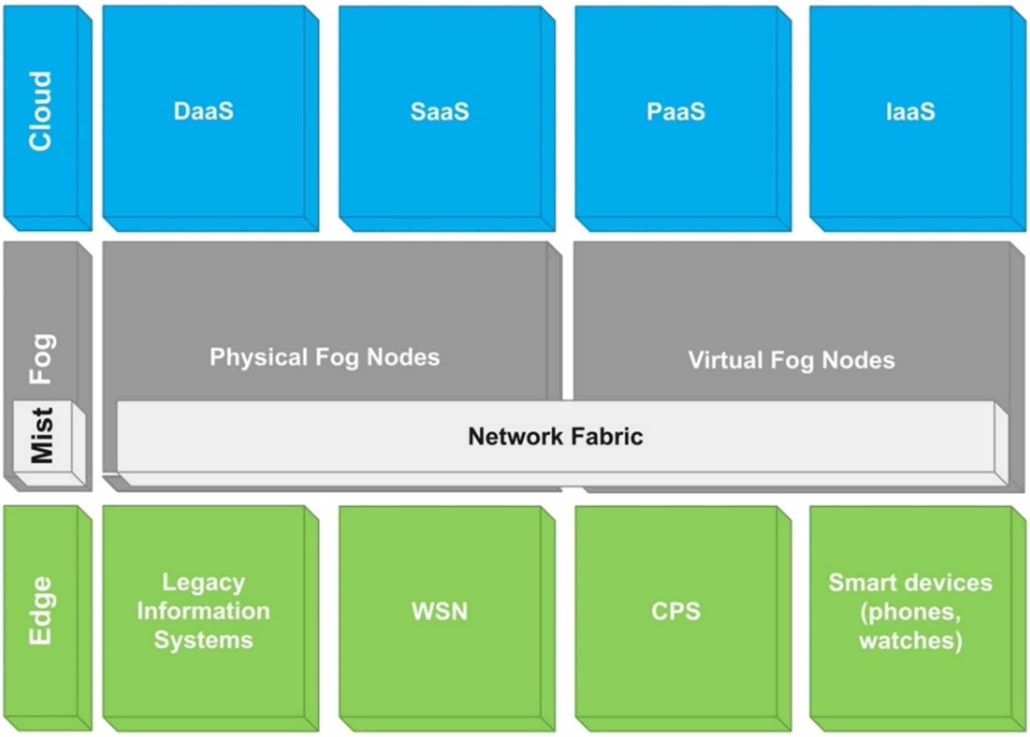

Figure 1. Layered view of the GHPE.

The layered consideration of GHPE described above provides the necessary abstraction to further study the challenges imposed toward designing an access control solution, placing the necessary components, and working on enhancing the operability of medical providers.

Finally, since resources are heterogeneous and dispersed, being stored in various locations using a set of different technologies, direct access can be quite challenging. To overcome this issue, the use of RAPs, as described in Section 2.4, in combination with VOs [59] can provide a unified platform for access control enforcement. Specifically, targeted RAPs can be developed for specific information system solutions by either using APIs or by being integrated into the software or any other solution used to manage resources. Moreover, VOs can be used in the case of IoMT devices where direct communication with devices is not possible and a sink node is used instead.

6. The Proposed Access Control Approach

The development of an access control solution for the GHPE should be based on a public, decentralized, and resilient platform. These characteristics can be satisfied by Ethereum, which is already globally available and provides the necessary technologies for the development of such an ACS.

6.1. Distributed Identities

As was already noted, and due to the versatile nature of the access control requirements in the GHPE, users need access to the system at any time and even without prior registration. In addition, the same person might undertake completely different roles depending on the environment he acts in. Hence, legacy access control approaches cannot satisfy these requirements. As a result, it is not viable to register every potential stakeholder to a central identity provider using a single unique identity which would also induce single-point-of-failure issues or be quick challenging in scaling. Identification through SSI [60] based on the use of verifiable claims that are held by the stakeholder and are verified by specific trusted authorities are proposed to be used. These authorities can be deployed to a national or multi-national extent and need to be trusted by any ecosystem member. Any stakeholder can present a convenient VC based on specific attributes and cryptographically verified by a trusted authority.

For example, when a patient comes to a healthcare provider asking for medical assistance, the consultant may need to access more information regarding the patient medical history or to access the patient's healthcare coverage by the concerned insurance company first. The healthcare provider, upon proving his eligibility for accessing the patient's information, can proceed with information retrieval and provision of the required service. In this case, there are several stakeholders and resources involved. The healthcare provider (e.g., a physician) should identify oneself by presenting a convenient claim that can be verified. Data holders, i.e., patients and insurance companies, should have the option to control access to information, and finally, information should be available to the requestor once the latter is authorized to access it.

6.2. NGAC in GHPE

NGAC uses discrete components for access requests and decision enforcement. Access requests are made against the PEP while enforcement is taking place in the RAP. To satisfy performance and availability requirements, the ecosystem includes multiple PEPs that can be placed in close vicinity to the requestors, existing mainly in the fog area [61]. This can be further improved by using IP anycast [62] addresses to ensure performance optimization and service availability. Moreover, PEPs can be integrated with client applications that are used by the users and can be provided from the cloud while using the SaaS model or via application programming interfaces where integration cannot be possible. Since NGAC supports both operational and administrative requests (the former is issued by the users while the latter is issued by the patients) that should be processed instantly, PEPs can also be placed in both the fog layer and the cloud. Placement in the fog includes medical facilities with multiple users to exploit the optimized performance characteristics of the fog, while the cloud provides availability for road warriors or autonomous users.

When a request is placed to a PEP, it is then forwarded to a PDP for evaluation. To reach a decision, PDP requires the full context, which includes the requestor, the resource and operation requested, as well as the defined relations (access control policies). While some information, such as the requestor, the operation, and the resource, are forwarded by the PEP, the PDP also needs to retrieve resource attributes and policy information. NGAC uses the PIP to store access control data. In a global environment, access control policies should be available throughout the GHPE where integrity and availability should be ensured. To achieve this goal, Ethereum provides a suitable environment since it provides both characteristics including availability and immutability properties of the blockchain.

When a decision is to grant access, PDP needs to notify the respective RAP if a resource is involved or the distributed PAP if an administrative operation has been requested. RAP is resource specific and, thus, it is proposed to be embedded in the resource or developed as a VO [59] that communicates with the resource. On the other hand, since policies are globally available and patients use PAP to perform administrative operations such as setting access control policies, PAP, in accordance, should also be distributed. PAP and RAP finally return execution status to the PDP which forwards it back to the requestor PEP, which in turn records access-related information using the EPP, which has a twofold role. Firstly, it logs access for the auditing needs, and secondly, it monitors the access session to change its state in the event of changes in attribute values dictated by the relative operation. Table 2 lists the placement of NGAC components among each layer of GHPE.

Table 2. NGAC components placement in GHPE layers.

Component	GHPE Layer	Details
PAP	Cloud	Provided as decentralized application that manages policies
PIP	Cloud/Fog	Includes policies stored in smart contracts
PDP	Fog	Implemented by smart contracts
PEP	Edge/Fog/Cloud	Located off-chain for stakeholders to enforce access control decisions and provide the means for stakeholders to request access
RAP	Mist/Edge	Resource-specific implementation to retrieve and store information as indicated by PEP
EPP	Cloud	Used to monitor access status and provide auditing

Figure 2 depicts the in-chain and off-chain deployment of NGAC components in the GHPE. PDP, PIP, and PAP are deployed in-chain either as smart contracts or decentralized applications, whereas other components are deployed off-chain. The user stands for the caregiver that requests access to patient data, for which the patient has previously manipulated access policies.

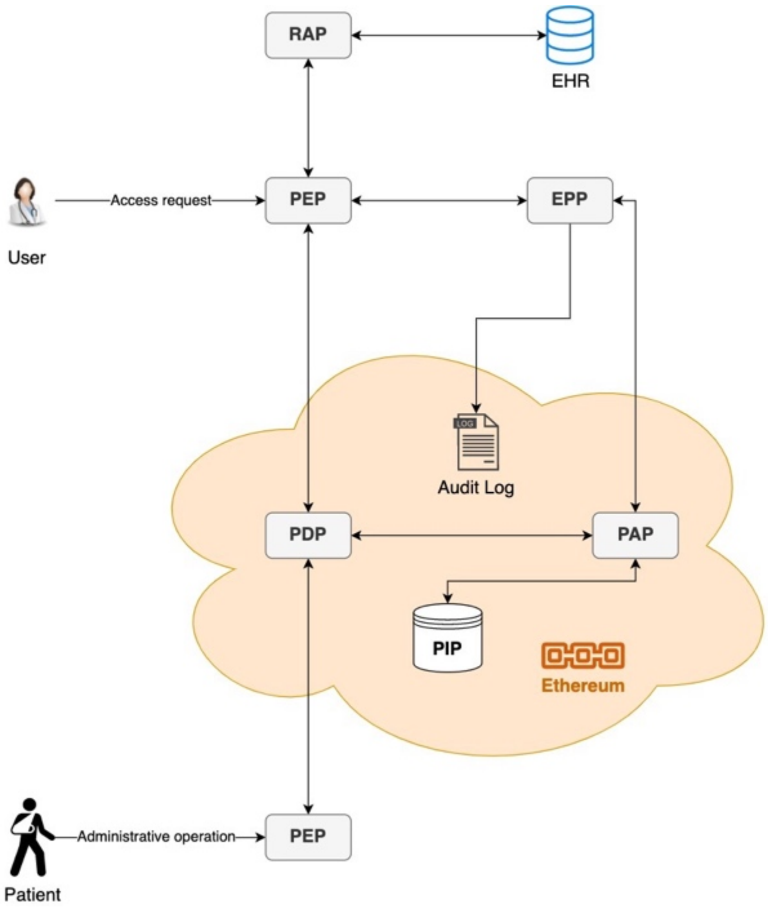

Figure 2. In-chain and off-chain deployment of NGAC components.

6.3. Smart Contracts

The use of smart contracts enables ACS in GHPE to implement attribute and policy stores where policy classes and attributes are immutable. For this purpose, we define three different types of smart contracts:

- The resource-holder smart contract (RSC). RSC is the means to store attribute values for the selected EHR as well as to provide the unique location of the resource payload. It can be considered as the agreement that defines the existence and validity of a resource. To mitigate privacy concerns, no medical information regarding the resource content is ever stored in this contract.
- The policy smart contract (PSC). PSC is generated by the patient himself the first time he needs to declare an access control policy (ACP) and is one per patient. It contains a set of policy classes that include the proper relations (as defined by NGAC) to form policies for a specific type or set of resources, which are not directly referred to but indirectly defined by the included containers (attributes). Specifically, each PSC contains the following: policy classes formed by relations that can be drilled down as tuples, obligations that define operational conditions, such as environmental attribute values, that need to be matched for the access to be permitted, and prohibitions to include privilege exceptions when certain conditions apply that cannot be described otherwise. When a patient needs to add, edit, or delete any policy classes, the whole contract is deprecated, and a new PSC is created instead.
- The decision-engine smart contract (DSC) is also required. It is used to reach access control decisions by calling the PSCs related to the patient identity presented and relatively requested resource RSCs to obtain attributes. DSC is executed by a PDP when a decision needs to be evaluated. Specifically, the PDP, being implemented as a decentralized application, receives a transaction including a requested resource, the

operation, and all user attributes in the form of VC. To determine access decision, PDP needs to evaluate the combination of policy classes as well as obtain the whole access request context (resource attributes and environmental attributes required). In terms of NGAC, DSC implements the concept of a decentralized PDP.

Although resource attributes do exist in the blockchain as in-chain data stored in RSC, environmental attributes are off-chain data that PDP needs to retrieve. Ethereum provides the mechanism for off-chain data retrieval, called oracles [63], which enables DSC to interact using APIs and query real-world information to retrieve all necessary attributes. All transactions and events processed by EPP are stored in the blockchain to form a detailed audit log. The interaction between smart contracts, applications, and environments is depicted in Figure 3.

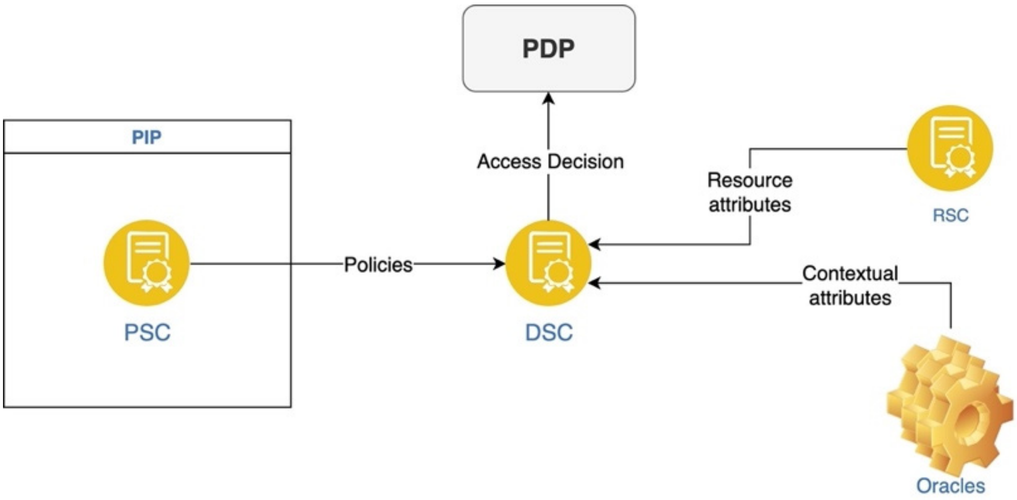

Figure 3. Interaction between the three types of smart contracts and the oracles.

6.4. GHPE Access Control Workflows

In legacy access control systems, a user should have been registered against an identity provider, authenticated, and then request access to objects (medical records) that according to the policy imposed would be granted or not. Access requests may need to be performed against different systems in various locations, which would further delay access and medical care, as a result. One may also find out that in the scenario above, caregivers and surgeons are completely unknown, and it would be preferable to obtain access granted to all possible life-saving information in an actual life-threatening scenario, whilst in any other case, this access would have been probably denied. Hence, decisions would be very much dependent on the context rather than the identity of the requesting person. Nevertheless, any access should be logged, so that any misuse would be discoverable by tracing.

We distinguish between two different types of workflows to present how authorization works in the GHPE. Access control administrative operations are used in controlling policy management when new records are created, while runtime operations implement authorization against various EHR resources when access is requested. In the GHPE, administrative operations are requested by patients and runtime operations are requested by users. These workflows are depicted as use cases in Figure 4.

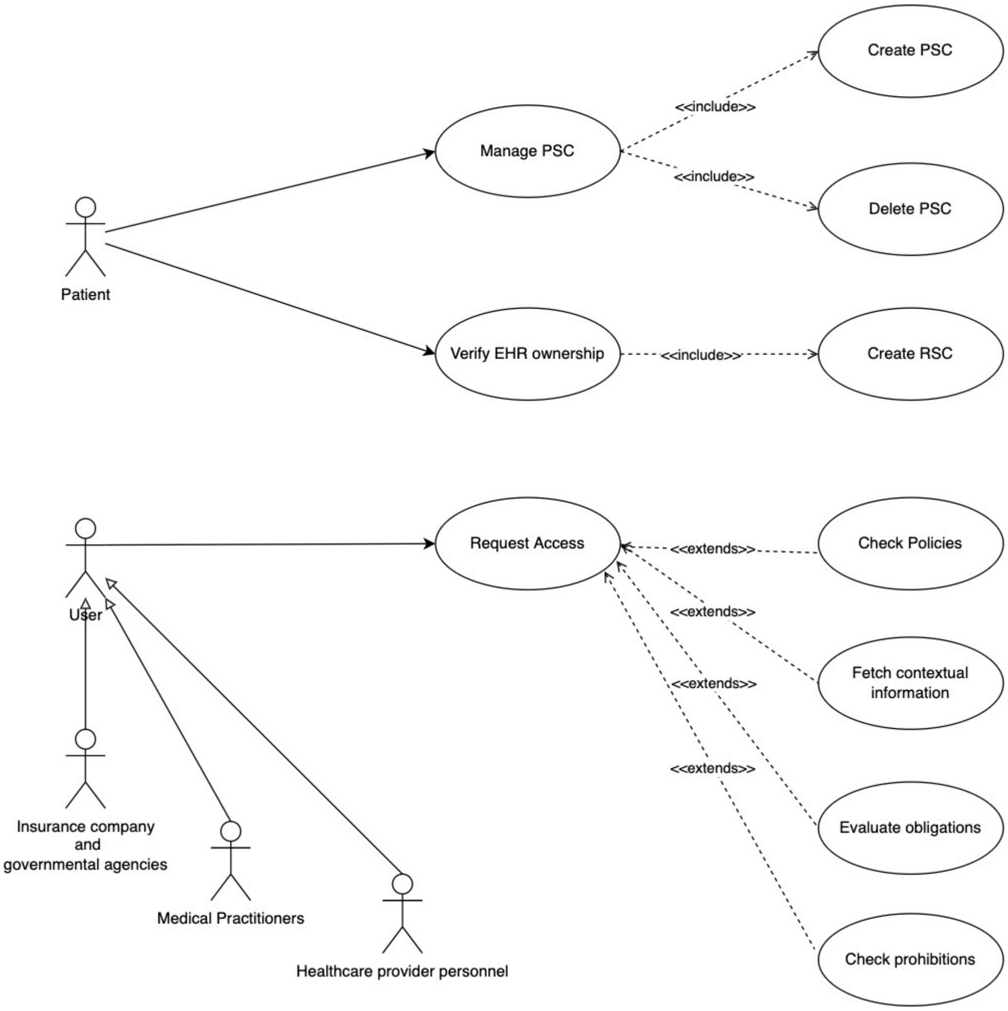

Figure 4. Use Cases of Access Control in GHPE.

6.4.1. Administrative Operations

When a new EHR is created or a device is deployed for a patient, the patient is notified via a smartphone application. Initially, the patient needs to verify the ownership of the record. Once he does, a new RSC is created and stored in the blockchain. The patient is then presented with existing policy classes stored in the PSC and has the option to review access control rules that derive from policy classes and affect the newly created EHR. The patient then can further manipulate policies by adding, editing, or deleting policy classes. If the new set of policy classes that apply to the record is different from the ones existing in the PSC, due to the immutability nature of the blockchain, the old PSC needs to be deprecated, and a new one will be stored instead. Since any decision is based on resource attributes rather than the resource ID, a small set of policy classes can control access to many records.

6.4.2. Runtime Operations

When the patient needs any kind of medical assistance, the users who need to gain prompt access to EHR (e.g., hospital personnel who check insurance data, caregivers providing first aid during his first visit, the ambulance caregivers, and the ECU personnel) place their access requests against the nearest PEP. In the case of hospital admissions and caregivers, PEPs can be integrated into a software package or be contacted by using an API, while in the ambulance case, PEP can be integrated into any SaaS application delivered from the cloud or be reached by a mobile app used in the ambulance.

Access request and decision making involve:

1. User contacts the nearest PEP to request access. Each access request includes the presented SSI, which includes user attributes, requested privileges, and target resources.
2. PEP forwards the request to a PDP for evaluation. PDP is deployed in-chain and is implemented by the PSC.
3. PDP needs to collect policies and attributes. For the former, it does so by contacting the PIP which is implemented by the PSC. Resource and contextual attributes are collected by the RSC in-chain and oracles off-chain, respectively.
4. If the decision is to allow access, PDP informs PEP and provides the resource location.
5. EPP ensures that no prohibitions exist, and obligations are met.
6. PEP fetches resource data (EHR) from the respective PAP and returns it to the user.
7. Throughout the access session, EPP keeps ensuring that obligations are met, or else the access session is dropped.

The access request decision-making flow is presented in Figure 5. If access is denied, the response is propagated back to the PEP for user notification. On the contrary, if access is permitted, the RAP that handles the specific resource is contacted and instructed to retrieve the EHR. RAP can be either integrated into the respective datastore located in the fog or edge area or be integrated into a VO that represents physical objects such as IoMT devices and sinks. RAP that can exchange data with the proprietary system or application that hosts the EHR fetches and delivers the information. It is worth mentioning that access decision is not a one-off process. Until access is complete, the decision is constantly re-evaluated throughout usage time and can be revoked at any time. For this reason, the EPP, apart from auditing, also ensures that if obligations are not met or any prohibition is applicable at any time throughout the access session, further access is denied. Figure 6 depicts in more detail the lifecycle of an access request as handled by the ACS.

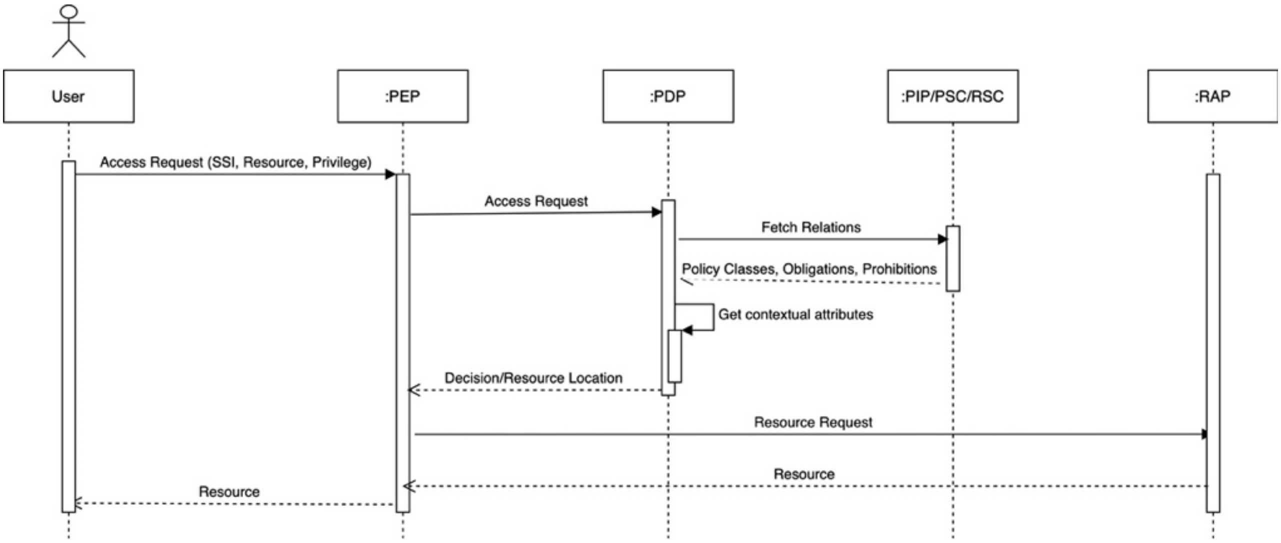
User
:PEP
:PDP
:PIP/PSC/RSC
:RAP
Access Request (SSI, Resource, Privilege)
Access Request
Fetch Relations
Policy Classes, Obligations, Prohibitions
Get contextual attributes
Decision/Resource Location
Resource Request
Resource
Resource

Figure 5. Access request and decision-making flow.

Specifically, when an access request is received (Step 1), user attributes are extracted (Step 2), and blockchain is queried to find and retrieve the PSC (Step 3). If a PSC is not available, then access is denied. Otherwise, obligations that are included in the PSC are checked (Step 4) to determine if any contextual attributes need to be fetched by the oracles (Step 5) to complete the full access request context. Then, policies included in PSC are evaluated (Step 6) to decide if access should be allowed. In the case when access is allowed, prohibitions are also checked (Step 7). If there are any prohibitions applicable, then access is denied. Otherwise, access is permitted (Step 8), and a new access session is established (Step 9). Throughout the session, obligations are constantly checked (Step 10) and anytime during the session when any obligation is not met, access will be immediately denied.

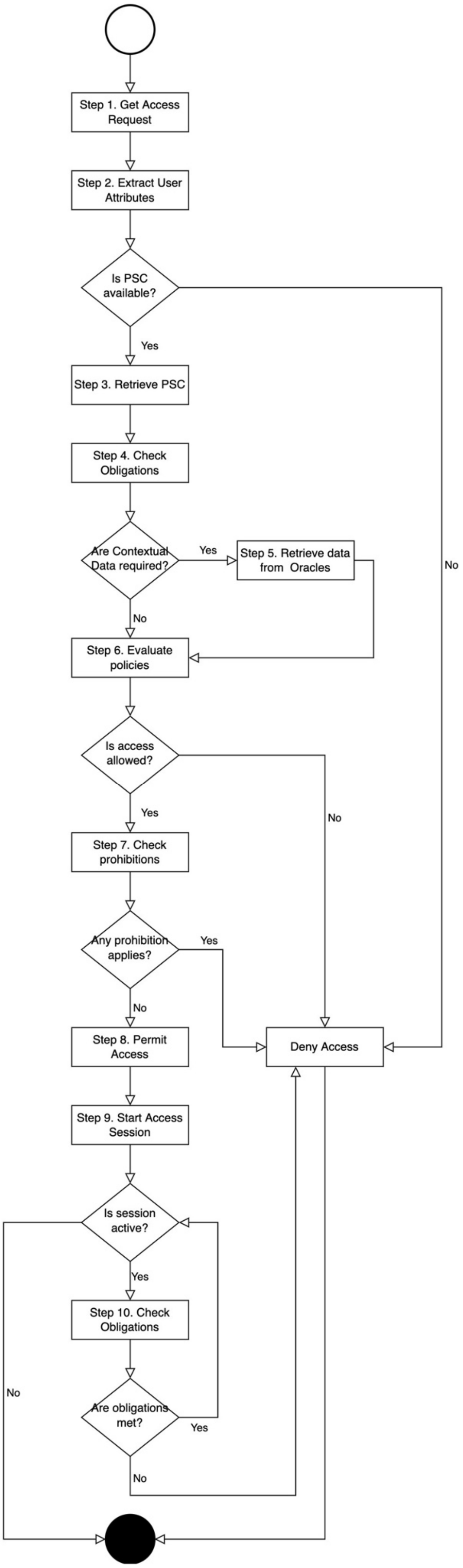
Step 1. Get Access Request
Step 2. Extract User Attributes
Is PSC available?
Yes
No
Step 3. Retrieve PSC
Step 4. Check Obligations
Are Contextual Data required?
Yes
Step 5. Retrieve data from Oracles
No
Step 6. Evaluate policies
Is access allowed?
Yes
No
Step 7. Check prohibitions
Any prohibition applies?
Yes
No
Step 8. Permit Access
Deny Access
Step 9. Start Access Session
Is session active?
Yes
No
Step 10. Check Obligations
Are obligations met?
Yes
No

Figure 6. Access request lifecycle.

7. Application Paradigm

Bob is a patient who has been using the smartphone application via which he can control access to his EHR including his medical history, previous diagnostic exams, and wearable devices' data, for health monitoring. The application is provided by a healthcare provider (HPU). Moreover, Bob, in his digital wallet, holds a set of VCs that he can selectively either use to perform access control administrative operations to define access policies regarding his EHR or present them to medical and insurance providers when he receives healthcare services.

During his latest travel, Bob suffered a health issue and drove to the nearest medical center to receive some assistance. Lisa, a secretary, who belongs to the admission personnel and is responsible for user admission, was able to check his insurance records while Bob did not have to carry any other documents or proofs of any type. He just used his digital wallet to provide the necessary attributes, which were extracted from his VC. The application used by the secretary performed a query in the blockchain to find the relative insurance records. Specifically, Lisa's application placed a request to the nearest PEP. The request included the secretary's VC, requested insurance records as the requested resources, and the read privilege. The PDP that received the request for evaluation needs to fetch resource attributes from the respective RSC and access control policy that derives from the policy classes in Bob's PSC.

Figure 7 depicts the related NGAC insurance policy class indicating that access is allowed to the secretary since there is a tuple "Admissions"—r—"Health Coverage" in policy class Insurance, and the resource "o4" is only associated in class Insurance. This leads to Lisa being allowed read access to health coverage data, since no obligation or prohibition stops her from doing otherwise. Therefore, since access to insurance records was allowed, and Bob was applicable, he was successfully admitted without any further delays.

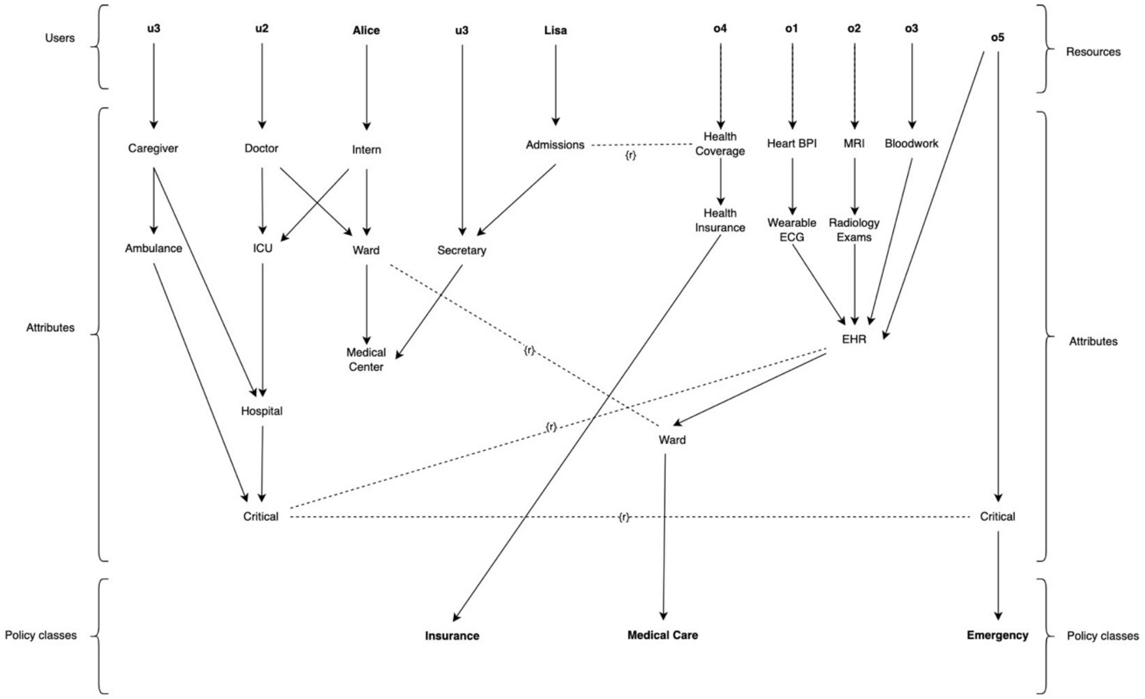

Figure 7. NGAC policy snapshot.

Alice is the intern doctor who afterwards examined Bob and found it necessary to ask for an MRI to be performed so she can be able to provide a better diagnosis for his condition. For simplicity, we assume that Alice performs and stores the exam, while in the real world, there would be more persons involved. When the exam is complete, Alice stores the outcome (images and diagnosis) in a PACS server [64] located in the data center of the medical center, which resides in the fog layer, and Bob is notified via the smart application that a new EHR is to be added. For this to happen, Bob should confirm that he has indeed undertaken the exam. When he does, a new RSC is created on his behalf that holds both the EHR location and all other attributes that can be used for access policy evaluation such as the type of the exam, the date, the medical center that performed it, etc. All other exam-specific data and metadata are not publicly available and are not stored anywhere in the blockchain. Moreover, Bob has the option to check how existing policies affect access to this new EHR and make any adjustments, if so required. This is necessary for the patient to be able to verify that the least required privileges are set.

For anyone to review the exam though, a PDP needs to evaluate permissions in combined policy classes. In the policy depicted in Figure 7, the MRI is contained in radiology exams, which in turn are contained in EHR. Alice as an intern has access to EHR only when she is in the ward, and access happens from within the ward. On the other hand, a hospital doctor can access EHR from everywhere.

When Alice reviews the exam, she finds out that she needs some further information regarding Bob's medical history. To obtain this information, she uses her terminal and requests access to Bob's recent bloodwork. Since Bob has already been admitted and resting in a ward, Alice is allowed access to the respective resources as depicted in the NGAC policy class Medical Care presented in Figure 7. Nevertheless, when Alice requests access to another resource, specifically the resource o5, access is denied. This happens because although the previous association still applies, o5 is also contained in policy class Emergency, for which there is no association between Alice and o5; that would only happen if Bob was in a critical state. Finally, after, a thorough examination and review, Alice permits Bob to exit the medical center but advises him to be very cautious and avoid any intense activity.

Unfortunately, some days later, Bob needs to be transferred by ambulance to the hospital. As GHPE users, caregivers in the ambulance can access the necessary EHR regarding Bob, as allowed by the association between Critical and EHR where the caregivers and the records are contained, respectively. Having the ability to obtain the information helps caregivers aid him in a better way and prepare hospital medical personnel for the incident. Bob is directed to the surgical room and the surgical team, and the ICU doctors afterward have full access to medical records and medical device readings which can be reached instantly. In this case, ambulance caregivers, as well as operating room personnel, are completely unknown to Bob, and all access decisions were based on user, resource, and contextual attributes, such as the condition of Bob. The permit decision is directed by the policy class Emergency that is also depicted in Figure 7 and is derived from the tuple u3-r-o5 existing in both medical care and emergency policy classes.

8. Discussion

In the application example presented in the previous section, Bob was able not only to receive prompt healthcare, but also to control access to his sensitive data. In addition, in the paradigm, there were various cases where access to resources was required under different circumstances. Specifically, resources such as insurance data, medical history, and even device readings, which are stored both on-premises and in the cloud, needed to be accessed. Users who requested access are the different persons in the medical center, in the hospital, in the ambulance, and maybe later in the insurance organization. Access control decision is determined by the decision context which includes user, resource, and environmental attributes that the PDP can obtain either on-chain or off-chain.

The decentralized nature of the proposed access control framework for the GHPE not only made it possible for all authorized users to access the data, regardless of their location, but eliminates any single-point-of-failure that would threaten the availability of the ACS. Likewise, no central storage for the EHR is required. Instead, the placement of the RAP component near the resources and the ability to develop customized RAPs suitable for any kind of datastore can realize the adaption of the proposed framework without requiring any major changes in current healthcare business operation.

DIDs allow the stakeholders to be responsible through the usage of the NGAC framework. To access resources, patients and users can select which identity to use. Depending on the selected identity ACS is provided with, the specific set of claims included in the presented identity and different access privileges can be enforced for different identities of the same person depending on the decision context and the policies configured. In the case of an emergency, such as the one presented in the scenario, medical caregivers can also have prompt access to data, due to NGAC's ability to perform authorization operations not based on the identity, which in this case, as previously explained can be unknown, but to contextual values that can answer to questions such as where, how, what, when, etc. while legacy access control systems base decisions on who. So, even where a patient might not be able to provide access rights, this can also be pre-arranged in policy classes as in Figure 7 which contains the policy class Emergency.

NGAC has the advantage of making the expression of security policies easy and the implementation of the access control able to be finely tuned over the layered technology consideration of GHPE. Furthermore, placing NGAC components in the GHPE layers between cloud, fog, mist, and edge, and in-chain and off-chain allocation, allows for a prompt and more reliable interaction between the components and the environment. Moreover, the usage of blockchain technology provides the necessary aspects of immutability, provenance, transparency, and auditability.

Administrative operations supported by NGAC is another feature that plays a significant and important role in the GHPE. In the scenario, Lisa, as HPU personnel, could easily identify Bob's insurance state and avoid time-consuming processes that may have had a negative impact on Bob's medical condition. Even if access might be firstly denied, Bob has the option to manipulate access policies himself, so any access rights can be sorted out in a timely manner and not having to contact any trusted third party. In the same manner, Alice, as the doctor, can suggest medical examinations and perform her duty without having to worry about providing access rights, since it can be all handled by the patient himself as well.

On the other hand, the blockchain which is being used for the deployment of some of the NGAC components still poses performance considerations such as those discussed in [65] The development and adaption of such an ecosystem and the access control framework proposed should require time and effort, both technically and administratively. Nevertheless, we strongly stand with the belief that the adaptation of such a solution given the fact that many performance issues regarding the blockchain are constantly being solved will be a key enabler of the vision of global healthcare provisioning.

9. Conclusions

In this paper, having identified the challenges in global healthcare provisioning and specified the layered technology consideration, which encounters various technical dependencies imposed, a set of access control requirements were specified. Then, a proposed orchestration of several state-of-the-art technologies and standards, such as distributed identities, blockchain technology, and NGAC are selected as the most prominent indispensable artifacts to be used.

Furthermore, placing NGAC components in the GHPE layers between cloud, fog, mist, and edge, and in-chain and off-chain allocation, provides the necessary flexibility in the adaption of the framework and finally more reliable access control. Finally, the usage of blockchain technology provides the necessary aspects of immutability, provenance, transparency, and auditability. All the above are complemented with the flexibility of various network architectures and the abstractions that are appropriate to deal with GHPE.

Author Contributions: Conceptualization, S.S. and I.M.; methodology, S.S., M.K., T.M. and I.M.; writing—original draft preparation, S.S. and M.K.; writing—review and editing, S.S., M.K., T.M. and I.M.; visualization, S.S.; supervision, I.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 457–464. [CrossRef]
2. Al-Sarawi, S.; Anbar, M.; Abdullah, R.; Hawari, A.B.A. Internet of Things Market Analysis Forecasts, 2020–2030. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 449–453. [CrossRef]
3. Joyia, G.J.; Liaqat, R.M.; Farooq, A.; Rehman, S. Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain. *J. Commun.* **2017**, *12*, 240–247. [CrossRef]
4. Fernández-Caramés, T.M.; Froiz-Míguez, I.; Blanco-Novoa, O.; Fraga-Lamas, P. Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care. *Sensors* **2019**, *19*, 3319. [CrossRef]
5. Li, C.; Hu, X.; Zhang, L. The IoT-based heart disease monitoring system for pervasive healthcare service. *Procedia Comput. Sci.* **2017**, *112*, 2328–2334. [CrossRef]
6. Villegas, D.; Martínez, A.; Quesada-López, C.; Jenkins, M. IoT for Cancer Treatment: A Mapping Study. In Proceedings of the 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 24–27 June 2020; pp. 1–6. [CrossRef]
7. Kim, J.H. 6G and Internet of Things: A survey. *J. Manag. Anal.* **2021**, *8*, 316–332. [CrossRef]
8. Di Renzo, M.; Zappone, A.; Debbah, M.; Alouini, M.-S.; Yuen, C.; de Rosny, J.; Tretyakov, S. Smart Radio Environments Empowered by Reconfigurable Intelligent Surfaces: How It Works, State of Research, and The Road Ahead. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2450–2525. [CrossRef]
9. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Tech. Rev.* **2021**, 1–14. [CrossRef]
10. Zhu, J.; Chan, D.S.; Prabhu, M.S.; Natarajan, P.; Hu, H.; Bonomi, F. Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture. In Proceedings of the 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, San Francisco, CA, USA, 25–28 March 2013; pp. 320–323. [CrossRef]
11. Flaumenhaft, Y.; Ben-Assuli, O. Personal health records, global policy and regulation review. *Health Policy* **2017**, *122*, 815–826. [CrossRef]
12. Directorate-General for Health and Food Safety. eHealth: Digital Health and Care. Available online: https://health.ec.europa.eu/ehealth-digital-health-and-care_en (accessed on 15 June 2022).
13. van Velthoven, M.H.; Cordon, C.; Challagalla, G. Digitization of healthcare organizations: The digital health landscape and information theory. *Int. J. Med. Inform.* **2019**, *124*, 49–57. [CrossRef]
14. Kahani, N.; Elgazzar, K.; Cordy, J.R. Authentication and Access Control in E-Health Systems in the Cloud. In Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; pp. 13–23. [CrossRef]
15. Ferraiolo, D.; Chandramouli, R.; Kuhn, R.; Hu, V. Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). In Proceedings of the 2016 ACM International Workshop on Attribute Based Access, New Orleans, LA, USA, 11 March 2016; pp. 13–24. [CrossRef]
16. Heart, T.; Ben-Assuli, O.; Shabtai, I. A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. *Health Policy Technol.* **2017**, *6*, 20–25. [CrossRef]
17. Salonikias, S.; Gouglidis, A.; Mavridis, I.; Gritzalis, D. *Access Control in the Industrial Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 95–114. ISBN 9783030057336.
18. Tolone, W.; Ahn, G.-J.; Pai, T.; Hong, S.-P. Access control in collaborative systems. *ACM Comput. Surv.* **2005**, *37*, 29–41. [CrossRef]
19. Bellare, M.; Rogaway, P. Entity Authentication and Key Distribution. In *Advances in Cryptology—CRYPTO' 93*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 232–249.
20. Liu, J.; Xiao, Y.; Chen, C.L.P. Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592. [CrossRef]

21. Manoj, T.; Makkithaya, K.; Pham, D.T.; Narendra, V.G. A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records. *Cogent Eng.* **2022**, *9*, 2035134. [CrossRef]
22. Brunner, C.; Gallersdörfer, U.; Knirsch, F.; Engel, D.; Matthes, F. DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. In Proceedings of the 3rd International Conference on Blockchain Technology and Applications (ICBTA 2020), Xi'an, China, 14–16 December 2020; pp. 61–66. [CrossRef]
23. Su, Y.; Wu, J.; Long, C.; Wei, L. Secure Decentralized Machine Identifiers for Internet of Things. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, Hilo, HI, USA, 12–14 March 2020; pp. 57–62. [CrossRef]
24. Belchior, R.; Putz, B.; Pernul, G.; Correia, M.; Vasconcelos, A.; Guerreiro, S. SSIBAC: Self-Sovereign Identity Based Access Control. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2021; pp. 1935–1943. [CrossRef]
25. Samarati, P.; de Vimercati, S.C. Foundations of Security Analysis and Design, Tutorial Lectures. *Lect. Notes Comput. Sci.* **2001**, *2171*, 137–196. [CrossRef]
26. Sandhu, R.; Samarati, P. Authentication, access control, and audit. *ACM Comput. Surv.* **1996**, *28*, 241–243. [CrossRef]
27. Hu, V.C.; Ferraiolo, D.F.; Kuhn, D.R. *Assessment of Access Control Systems*; NIST Interagency/Internal Report (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2006.
28. Kayes, A.S.M.; Kalaria, R.; Sarker, I.H.; Islam, M.S.; Watters, P.A.; Ng, A.; Hammoudeh, M.; Badsha, S.; Kumara, I. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. *Sensors* **2020**, *20*, 2464. [CrossRef]
29. Hu, V.C.; Kuhn, D.R.; Ferraiolo, D.F.; Voas, J. Attribute-Based Access Control. *Computer* **2015**, *48*, 85–88. [CrossRef]
30. Alshehri, A.; Sandhu, R. Access Control Models for Virtual Object Communication in Cloud-Enabled IoT. In Proceedings of the 2017 IEEE International Conference on Information Reuse and Integration (IRI), San Diego, CA, USA, 4–6 August 2017; pp. 16–25. [CrossRef]
31. Monrat, A.A.; Schelen, O.; Andersson, K. A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
32. Patel, D.; Bothra, J.; Patel, V. Blockchain Exhumed. In Proceedings of the 2017 ISEA Asia Security and Privacy, Surat, India, 29 January–1 February 2017; pp. 1–12. [CrossRef]
33. Elangovan, D.; Long, C.S.; Bakrin, F.S.; Tan, C.S.; Goh, K.W.; Yeoh, S.F.; Loy, M.J.; Hussain, Z.; Lee, K.S.; Idris, A.C.; et al. The Use of Blockchain Technology in the Health Care Sector: Systematic Review. *JMIR Med. Inform.* **2019**, *10*, e17278. [CrossRef] [PubMed]
34. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain Technology Use Cases in Healthcare. In *Advances in Computers*; Raj, P., Deka, G.C., Eds.; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41. [CrossRef]
35. Adler, J.; Berryhill, R.; Veneris, A.; Poulos, Z.; Veira, N.; Kastania, A. Astraea: A Decentralized Blockchain Oracle. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1145–1152. [CrossRef]
36. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. FairAccess: A new Blockchain-based access control framework for the Internet of Things: FairAccess: A New Access Control Framework for IoT. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
37. Satamraju, K.P.; Malarkodi, B. Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare. *Sensors* **2020**, *20*, 1389. [CrossRef]
38. Ali, A.; Rahim, H.A.; Ali, J.; Pasha, M.F.; Masud, M.; Rehman, A.U.; Chen, C.; Baz, M. A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority. *Appl. Sci.* **2021**, *11*, 9999. [CrossRef]
39. Kumar, R.; Tripathi, R. Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model. *J. Ambient Intell. Humaniz. Comput.* **2020**, *12*, 2321–2338. [CrossRef]
40. Albreiki, H.; Alqassem, L.; Salah, K.; Rehman, M.H.; Svetinovic, D. Decentralized Access Control for IoT Data Using Blockchain and Trusted Oracles. In Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 11–12 November 2019; pp. 248–257. [CrossRef]
41. Hossein, K.M.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Comput. Commun.* **2021**, *180*, 31–47. [CrossRef]
42. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. *J. Med. Internet Res.* **2020**, *22*, e13598. [CrossRef] [PubMed]
43. Mubarakali, A.; Bose, S.C.; Srinivasan, K.; Elsir, A.; Elsier, O. Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–9. [CrossRef]
44. Alsayegh, M.; Moulahi, T.; Alabdulatif, A.; Lorenz, P. Towards Secure Searchable Electronic Health Records Using Consortium Blockchain. *Network* **2022**, *2*, 239–256. [CrossRef]
45. Younis, M.; Lalouani, W.; Lasla, N.; Emokpae, L.; Abdallah, M. Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. *IEEE Syst. J.* **2021**, *99*, 1–12. [CrossRef]
46. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* **2022**, *164*, 152–167. [CrossRef]

47. Cong, R.; Liu, Y.; Tago, K.; Li, R.; Asaeda, H.; Jin, Q. Individual-Initiated Auditable Access Control for Privacy-Preserved IoT Data Sharing with Blockchain. In Proceedings of the 2021 IEEE International Conference on Communications Workshops, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. [CrossRef]
48. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management. *IEEE Trans. Comput. Soc. Syst.* **2022**, 1–13. [CrossRef]
49. Geetha, V.; Balakrishnan, B. A User Authentication and Access Control Scheme for IoT-Based Healthcare Using Blockchain. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies, Kharagpur, India, 6–8 July 2021; pp. 1–7. [CrossRef]
50. Abowd, G.D.; Dey, A.K.; Brown, P.J.; Davies, N.; Smith, M.; Steggles, P. Towards a Better Understanding of Context and Context-Awareness. In Proceedings of the International Symposium on Handheld and Ubiquitous Computing, Karlsruhe, Germany, 27–29 September 1999; Volume 1707, pp. 304–307. [CrossRef]
51. Alhaqbani, B.; Fidge, C. Business Process Management Workshops. *Lect. Notes Comput. Sci.* **2008**, *100*, 371–382. [CrossRef]
52. Beznosov, K.; Inglesant, P.; Lobo, J.; Reeder, R.; Zurko, M.E. Usability Meets Access Control: Challenges and Research Opportunities. In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, Stresa, Italy, 3–5 June 2009; pp. 73–74. [CrossRef]
53. Rostad, L.; Edsberg, O. A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs. In Proceedings of the 2006 22nd Annual Computer Security Applications Conference, Miami Beach, FL, USA, 11–15 December 2006; pp. 175–186. [CrossRef]
54. Weiser, M. The computer for the 21st century. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **1999**, *3*, 3–11. [CrossRef]
55. Sandhu, R.; Samarati, P. Access control: Principle and practice. *IEEE Commun. Mag.* **1994**, *32*, 40–48. [CrossRef]
56. McCann, J.; Quinn, L.; McGrath, S.; O'Connell, E. Towards the Distributed Edge—An IoT Review. In Proceedings of the 2018 12th International Conference on Sensing Technology, Limerick, Ireland, 4–6 December 2018; pp. 263–268. [CrossRef]
57. Iorga, M.; Feldman, L.; Barton, R.; Martin, M.J.; Goren, N.; Mahmoudi, C. *Fog Computing Conceptual Model*; NIST Special Publication 500-325; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
58. Yogi, M.K.; Chandrasekhar, K.; Kumar, G.V. Mist Computing: Principles, Trends and Future Direction. *Int. J. Comput. Sci. Eng.* **2017**, *4*, 19–21. [CrossRef]
59. Alshehri, A.; Sandhu, R. Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda. In Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, Pittsburgh, PA, USA, 1–3 November 2016; pp. 530–538. [CrossRef]
60. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
61. Salonikias, S.; Mavridis, I.; Gritzalis, D. *Access Control Issues in Utilizing Fog Computing for Transport Infrastructure*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 15–26.
62. Metz, C. IP anycast point-to-(any) point communication. *IEEE Internet Comput.* **2002**, *6*, 94–98. [CrossRef]
63. Al Zaabi, A.; Yeun, C.Y.; Damiani, E. Trusting Testcases Using Blockchain-Based Repository Approach. *Symmetry* **2021**, *13*, 2024. [CrossRef]
64. Strickland, N.H. Current topic: PACS (picture archiving and communication systems): Filmless radiology. *Arch. Dis. Child.* **2000**, *83*, 82–86. [CrossRef] [PubMed]
65. Jović, M.; Filipović, M.; Tijan, E.; Jardas, M. A Review of Blockchain Technology Implementation in Shipping Industry. *Pomorstvo* **2019**, *33*, 140–148. [CrossRef]