# Blockchain-enabled Next Generation Access Control

**Yibin Dong[1], Seong K. Mun[1], Yue Wang[1]**

[1] Virginia Polytechnic Institute and State University, Arlington VA 22203, USA

yibin.dong@vt.edu, munsk@vt.edu, yuewang@vt.edu

**Abstract** In the past two decades, longitudinal personal health record (LPHR) adoption rate has been low in the United States. Patients' privacy and security concerns was the primary negative factor impacting LPHR adoption. Patients desire to control the privacy of their own LPHR in multiple information systems at multiple facilities. However, little is known how to model and construct a scalable and interoperable LPHR with patient-controlled privacy and confidentiality that preserves patients' health information integrity and availability. Understanding this problem and proposing a practical solution are considered important to increase LPHR adoption rate and improve the efficiency as well as the quality of care. Even though having the state-of-the-art encryption methodologies being applied to patients' data, without a set of secure access control policies being implemented, LPHR patient data privacy is not guaranteed due to insider threats. We proposed a definition of "secure LPHR" and argued LPHR is secure when the security and privacy requirements are fulfilled through adopting an access control security model. In searching for an access control model, we enhanced the National Institute of Standards and Technology (NIST) next generation access control (NGAC) model by replacing the centralized access control policy database with a permissioned blockchain peer-to-peer database, which not only eases the race condition in NGAC, but also provides patient-managed access control policy update capability. We proposed a novel blockchain-enabled next generation access control (BeNGAC) model to protect security and privacy of LPHR. We sketched BeNGAC and LPHR architectures and identified limitations of the design. **Keywords:** Secure LPHR, Blockchain-enabled Next Generation Access Control, Privacy, Confidentiality, Security

## 1. Introduction

The longitudinal personal health record (LPHR) is "an electronic, lifelong resource of health information needed by individuals to make health decisions"[1] and to "improve the quality and efficiency" of their own health care[2]. There are three types of personal health record (PHR) implementations: standalone PHR, tethered PHR, and untethered[3] PHR.

- *Standalone PHR* is managed by patients without health care providers' inputs [4].Patients have full control of data in a standalone PHR. However, standalone PHR is not connected to any of the electronic health record (EHR) systems[4].
- *Tethered PHR* is confined in a single EHR system[3]. In this setting, patients and providers form a partnership. Patients are allowed to directly access their clinical data with read-only permission. Additionally, patients can request to add supplementary information to their own patient records. The hosting health care provider of the tethered PHR has full control of the patient records[4].
- When patients receive care from multiple providers that use different EHRs, a cross-organizational PHR or integrated non-tethered PHR or *untethered PHR* is required to provide a complete patient PHR dataset[3]. There has been more interest to develop untethered PHR due to its capability of building longitudinal patient health records[3]. Furthermore, patients showed strong interest in untethered PHR, with expectations of easy access to a centralized PHR system and full control of their own PHR[4], where patients, providers, payers, and stakeholders are sharing the same platform[3].

Digitizing patients' medical records was started and mandated in "the Health Insurance Portability and Accountability Act of 1996 (HIPAA)"[5]. One of the objectives of HIPAA was "to simplify the administration of health insurance."[6] that led to use of EHR. The first HIPAA Privacy Rule was released[5] to "improve privacy standards and to restrict the disclosure of Protected Health Information (PHI) and personal identifiers to unauthorized individuals"[5]. There was no incentive to use untethered PHRs to build LPHR[7] at that time. To promote implementations of EHR and fix a loophole in the HIPAA privacy rule, "the Health Information Technology for Economic and Clinical Health Act" ("the HITECH Act") was enacted"[8] with PHR adoption incentives. However, despite the U.S. federal government's laws and regulations, including incentives and penalties, LPHR adoption rate has been low (Figure 1) in the past two decades[9, 10]. A.A. Abd-alrazaq et al conducted a comprehensive PHR literature review of peer-reviewed publications between 2000 and 2018 and concluded patients' privacy and security concerns was the primary negative factor[9]. Moreover, health care providers are using some type of EHR systems that are managed by various EHR vendors. Hence patients' health care records can be scattered in different information systems at various facilities. Patients showed strong interest in untethered PHR with expectations of easy access to and full control of their own LPHR [4]. Patients want to be assured that nobody can access their LPHR without patients' authorization[9]. Furthermore, on March 9, 2020, "the ONC Cures Act Final Rule"[11] and "the CMS Interoperability and Patient Access Final Rule"[12] were released to truly give patients authority to control access to their health care data. However, little is known how to model and construct a scalable and interoperable LPHR with patient-controlled privacy and confidentiality that preserves patients' health information integrity and availability. This motivated us to research an ef-

fective novel design of secure LPHR that can ease the patients' security and privacy concerns in order to increase LPHR adoption rate in the Unites States.


**Fig.** "Office-based Physician Electronic Health Record Adoption (2004-2017)"[10]**.**

During reviewing works accomplished by peers from 1970 to 2020, we found encryption, which was used as the primary methodology to protect privacy and confidentiality of patients' data, could only prevent external risks but not insider threat[13]. A secure access control model along with implementation mechanism are desired to remediate internal threats. After analyzing LPHR requirements and both traditional as well as next generation access control models, we explained our preference of the National Institute of Standards and Technology (NIST) next generation access control (NGAC) model[14]. However, NGAC inherited a drawback of "race condition" from distributed systems. We overcame this by integrating permission blockchain Hyperledger Fabric (HF) with NGAC and reconstructed a novel blocked-enabled NGAC (BeNGAC) model. NGAC is also complementary to HF and boosts the HF confidentiality protection capability through next generation access control policies. The BeNGAC offers granular patient consent capability so it can improve the trustfulness between patients and providers who manage the untethered PHR. We sketched BeNGAC functional architecture as well as LPHR architecture. Key properties of BeNGAC were identified that can fulfill the requirements of a scalable and interoperable LPHR with patient-controlled privacy and confidentiality that preserves patients' health information integrity and availability. A high-level example of BeNGAC policy configuration was given to demonstrate the privacy protection capability of BeNGAC.

## 2. LPHR Privacy and Security Literature Review

This systematic review was conducted using instructions from the "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Statement"[15] to avoid publication selection bias[16]. Library worldwide union

catalog WorldCat[17] and Google Scholar were employed as the main searching tools. The search started on May 10th, 2020 and finished on May 23rd, 2020. The search terms were based on keywords: longitudinal [personal | patient] [health | medical] record [security | privacy | confidentiality]. Publications were chosen from year 1970 to 2020. Studies were excluded if they were not peer-reviewed to avoid selection bias[16]. Only English language was included in the search. The publications worldwide were included. 1,232 results in WorldCat libraries and 32 outcomes in Google Scholar were returned. Duplicated studies were excluded. After reviewing titles and abstracts, 23 peer-reviewed publications were chosen to conduct further analysis.

**Review Results:** Encryption was the primary approach to protect privacy and security from external threats. However, Miller & Tucker[13] conducted an empirical research of the relationship between patient data encryption and loss of data. The authors concluded applying encryption to patient data does not decrease proclaimed incidents of data loss. On the contrary, there were increased likelihood of public announcements of patient data loss because of human errors, from either computer equipment stolen or insider security threats. Miller & Tucker argued that vulnerability of misused privileges inside organizations are bigger than external threats. The authors recommended policymakers to expand the scope of security measure by including user access control which is more suitable than encryption to tackle the insider vulnerability or threat.

## 3. LPHR Requirements

A) **LPHR Security and Privacy**: LPHR security rules are developed to protect information system against intrusion, either intentional or by accident, while LPHR privacy rules are built to hide information from unauthorized people or processes. Patients' health information availability, integrity, and confidentiality are the core of LPHR security. Under the HIPAA Security Rule, LPHR availability means personal health records "are accessible and usable on demand by authorized persons"[18]. LPHR integrity means personal health records "are not altered or destroyed in an unauthorized manner"[18]. LPHR confidentiality, by its security definition, preventing unauthorized access and disclose of LPHR, serves as a means to protect patients' privacy so that patients' health information is not revealed to unauthorized subjects. Therefore, confidentiality is a property of both LPHR security and privacy. The HIPAA Security Rule's[18] confidentiality property of LPHR reinforces the privacy requirements in the HIPAA Privacy Rule, which disallow unauthorized use and disclosure of LPHR.

B) **LPHR Authorization:** LPHR consists of two independent components, standalone PHR and untethered PHR. A patient has control of both parts of the patient's health records stored in two partitions of the storage under different rules and regulations. The LPHR authorization requirements are summarized in *Table 1*.

**Other Requirements:** C) changes to LPHR are tamper resistant; D) access is fully auditable; E) LPHR is enterprise scalable; F) LPHR is distributed; G) LPHR is interoperable and integrable to other EHRs.

**Table 1.** LPHR Authorization.

| LPHR Patients' Data Source | Patients' Permission | LPHR Providers' or Administrators' Permission | Third Parties' Permission |
|---|---|---|---|
| Data Generated by Patients | Full control | Manage on behalf of patient upon patients' authorization | Can request to access individuals' information with patients' authorization. |
| Patients' EHR Data in Covered Entity | Read | Disclose to patients' LPHR with patients' authorization | Can request to access individuals' information with patients' authorization. |
| Untethered PHR providers (or covered entities) | Read access.<br>Can request to submit supplemental information to be added to PHR.<br>Can control access to the patients' PHR by third parties.<br>Can control access to the patients' PHR by the covered entities of the untethered PHR. | Can use individuals' PHI permitted by HIPAA Privacy Rule.<br>Can disclose individuals' PHI to third parties permitted by HIPAA Privacy Rule. | Can request to access individuals' information with patients' authorization. |

## 4. System Design and Methods

Access control model is a formal representation of access control policies and their implementation reinforcement mechanisms on the systems being designed[19]. "By proving the access control model is secure (w.r.t. meeting the policies compliance requirements), demonstrating the model is correctly implemented through access control mechanisms which fulfil the security requirements, we can convince users and vendors that the system adopting the access control model is secure"[20, 21]. Hence, the LPHR adopted the secure access control model is a *secure LPHR*.

There are two categories of access control models. Traditional access control model is established on a closed centrally controlled and server-oriented access control environment, in which users are well-known[22]. "Discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC)"[19] belong to traditional access control model. Next generation access control model is based on open access control surroundings, where users can be unknown or centrally known. "Attribute-based access control (ABAC)"[19] is next generation access control model. The NIST NGAC, a type of ABAC, was

standardized by the "InterNational Committee for Information Technology Standards (INCITS)"[14]. NGAC was chosen to construct secure LPHR because firstly, users of LPHR can be unknown or centrally known, which fits the property of NGAC. Secondly, NGAC provides unifying access control policies while the resources reinforcing the access control polices locally are distributed[19], which aligns with data distributedness requirement of LPHR. Thirdly, NGAC is enterprise scalable[19] that fulfills the requirement of LPHR scalability. Lastly, NGAC model is "inherently policy neutral"[23] and applies to any users or objects that have common attributes described by a policymaker, which gives much flexibility when implementing in organizations.

However, in the NGAC model and the NIST Policy Machine[23] mechanism, since the decision making and policy expression are disjointed, it can cause a "race condition" in distributed systems[23]. We addressed this problem by replacing the NGAC policy database with a peer-to-peer decentralized blockchain database and reshaped the NGAC model to be BeNGAC. We chose "permissioned" blockchain HF[24] because it fits the property of LPHR that patients and providers forming a trusted network. The immutability of HF guarantees data integrity which is timestamped. Moreover, the "concurrency control"[25] in HF eases the race condition in NGAC model by utilizing the "HF consensus"[25]. The access control data is stored in off-chain private database, while the transactional audit logs are on-chain. On the other side, the data in HF is protected with little degree of confidentiality, and this can be perfected by NGAC access control policies. Commonly, both NGAC and HF are finite state machines[24, 26], which are naturally married together as a new model BeNGAC.

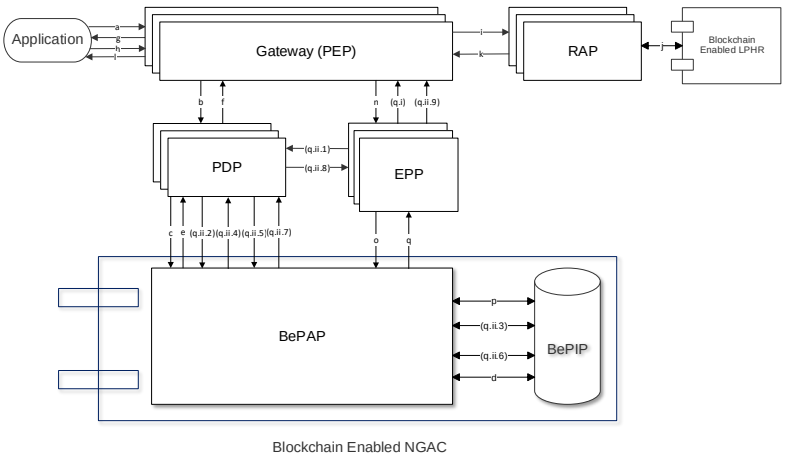


**Fig 2.** Blockchain-enabled NGAC Functional Architecture [23].

**BeNGAC Functional Architecture (Figure 2):** In this new model, resources ("policy enhancement point (PEP), policy decision point (PDP), event processing

point (EPP), resource access point (RAP), policy administration point (PAP), and policy information point (PIP)"[23]) forcing the access control policies are locally distributed. "PEP"[23] checks the authorization permissions via "PDP"[23], which queries the blockchain-enabled PIP (BePIP) policy database via blockchain-enabled PAP (BePAP). BePAP acts as an endorsing or committing peer along with BePIP are decentralized which constitute a BeNGAC policy administration unit. The applications accessing the same policy database share the identical BeNGAC policies. During "event response (obligation)" or "prohibition"[23], "EPP"[23] queries the same BeNGAC policy database BePIP.

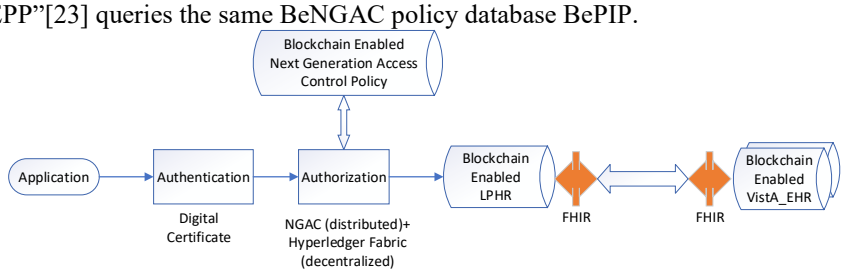


**Fig 3.** LPHR Architecture**.**

**LPHR Architecture (Figure 3):** A user accesses his or her LPHR through an application. The user is assigned with a digital certificate which is pre-generated by the certificate administrators. Upon successful authentication, the user is presented with a view of his or her own LPHR. This list of authorized view of information is retrieved from BeNGAC policy database.

The authentication via digital certificate governs the LPHR login security with the user's identity. The BeNGAC policy protects the LPHR from being "altered or destroyed in an unauthorized manner"[18], i.e. ensuring *LPHR integrity*. The policy also guarantees the LPHR "is accessible and usable on demand by an authorized person"[18], which provides *LPHR availability*. The policy disallows unauthorized use and disclosure of LPHR to unauthorized parties, which safeguards *LPHR confidentiality*. Therefore, with digital certificate guarded secure authentication and BeNGAC policies, we can meet the LPHR security and privacy as well as access authorization requirements, which include U.S. privacy policies, laws and regulations.

Unauthorized changes are prohibited by BeNGAC policies. This meets the tamper resistance change requirement. BeNGAC is enterprise scalable because both NGAC and HF are enterprise scalable[23, 24].

*Shared Access Control Policy Database:* the patient has full control of the permissions of his or her own records in the LPHR. A patient is able to give very granular consent to use their LPHR by trusted providers, which will improve the trustfulness between patients and providers. The access control information is stored in a dedicated BeNGAC database, which is distributed yet decentralized among trusted parties in a secure blockchain network. Any member in the patient's BeNGAC network share the same access control information that is updat-

ed in the order of timestamp which is tamper resistant and immutable. The changes are recorded in blockchain audit logs. The changes are non-repudiable. The blockchain based peer-to-peer BeNGAC database avoids racing condition during policy reinforcement.

The patients and health care providers are granted permissions to use the applicant client to access the HF network. The patient and one or more designated health care providers in the HF network are assigned with endorsing peer role. The patient and all health care providers in the HF network are committing peers.

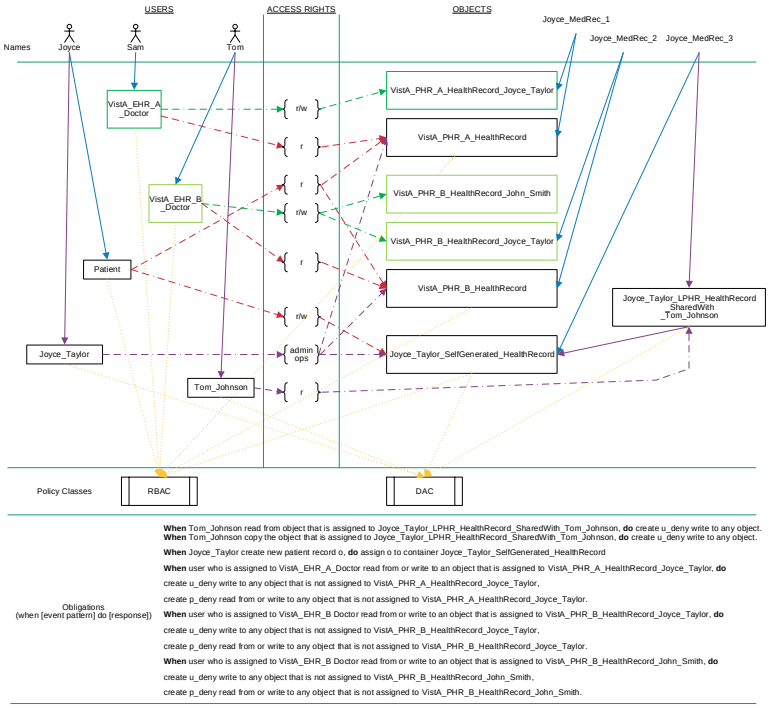


**Fig 4.** BeNGAC Policy Configuration**.**

An example of BeNGAC policy configuration has been provided in Figure 4 to illustrate the capability of privacy protection. In this implementation, from a patient point of view, the LPHR consists of three parts: patient health records stored in EHR VistA PHR A, patient health records contained in EHR VistA PHR B, and patient self-generated health records from personal devices or manual inputs. RBAC and DAC policy classes are governed by policy administrators. Two RBAC data leakage prevention obligation rules are configured:

**Configuration Rule 1:**

**When** process $p$ performs $(r, o)$ where $o \rightarrow med\_rec$ **do** create $u\_deny(p, \{w\}, \neg o)$

**Configuration Rule 2:**

**When** process $p$ performs $(copy, o)$ **do** create $u\_deny(p, \{w\}, \neg o)$

The derived privileges of the configuration are the following:
(Joyce,r,Joyce_MedRec_1),(Joyce,r,Joyce_MedRec_2),(Joyce,r,Joyce_MedRec_3),
(Joyce,w,Joyce_MedRec_3),(Sam,r,Joyce_MedRec_1),(Sam,w,Joyce_MedRec_1)
(Tom,r,Joyce_MedRec_2),(Tom,w,Joyce_MedRec_2),(Tom,r,Joyce_MedRec_3)

## 5. Discussions

There are few limitations of the design. Firstly, being the kernel of the security features offered by the LPHR, owner's secret private key is essential and the passport to manage his or her LPHR securely. All transactions are dependent on the secret private key for authentication. This security feature is inherited from the blockchain technology itself, and naturally the problem when the owner losing the private secret key presented a road blocker if there is no solution to this challenge.

Secondly, in general, LPHR owner can grant permissions to a legitimate third party, for instance a specialist doctor he or she will visit during a referral encounter. There are situations such as emergency departments visit, where LPHR access is desired by the ER physicians to make better decision of a care plan by using the patient's LPHR information such as medications taken, allergy conditions, recent doctors' visits, chronic diseases, and recent laboratory test results. However, as a limitation that the patient needs to directly grant the permissions of LPHR to the doctors in ER, it is not uncommon that the patient is unconscious and cannot authorize the access of his or her LPHR to the doctors in ER facility.

These two problems can be solved by using proposed BeNGAC model. The former incident is rare, so the recovery of the owner's private secret key can be purposely designed with a sophisticated and secure execution plan by using BeNGAC and RBAC separation of duty (SoD) [19] capability. The latter can be worked out by using BeNGAC and DAC policy.

In this research, we proposed a solution to ease the "privacy and security concerns of patients" [9] when adopting LPHR in the United States. We provided a formal definition of "secure LPHR" and introduced a novel BeNGAC model. We designed a scalable and interoperable LPHR with patient-controlled privacy and security. While "blockchain-based self-sovereign identity" [27] focuses on identity management (decentralized authentication), the proposed solution contributes to the knowledge by emphasizing granular patient-controlled decentralized authorization, which has gone beyond the trust of identity, i.e. governance of trust around confidentiality, availability, integrity, and privacy.

We are in the process of implementing the design and applying to a use case of patient data access control and platform sharing among providers. We are also developing a prototypical evaluation and plan to measure the properties of the design such as processing delay, security and privacy control, scalability, auditability, and tamper resistibility.

## References

1. AHIMA, *Defining the Personal Health Record.* Journal of AHIMA, 2005. **76**(6): p. 24-25.
2. *Personal Health Records and the HIPAA Privacy Rule*. [cited 2021 5/26]; Available from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

3. *Key considerations, Venesco and Personal Health Records Community of Practice*, in *Health Information Exchange (HIE) Shared Collaborative Learning Combine*. 2015, Venesco LLC.
4. Assadi, V., *Adoption of Integrated Personal Health Record Systems: A Self-determination Theory Perspective*, M. University, Editor. 2013: Hamilton, Ontario. p. 1-195.
5. *HIPAA history*. [cited 2021 5/17]; Available from: https://www.hipaajournal.com/hipaa-history/.
6. *Pub. L. No. 104-191, 110 Stat. 1936.* 1996.
7. Sterud, B., *PRACTITIONER APPLICATION: The Challenges in Personal Health Record Adoption.* J Healthc Manag, 2019. **64**(2): p. 109-110.
8. *H.R.1 - American Recovery and Reinvestment Act of 2009 PLAW-111publ5.* 2009.
9. Abd-Alrazaq, A.A., et al., *Factors that affect the use of electronic personal health records among patients: A systematic review.* Int J Med Inform, 2019. **126**: p. 164-175.
10. ONC, *Office-based Physician Electronic Health Record Adoption*. 2017: https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php.
11. *ONC Cures Act Final Rule*. March 9, 2020, ONC: https://www.healthit.gov/curesrule/.
12. *CMS Interoperability and Patient Access Final Rule*. March 9, 2020, CMS: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index.
13. Miller, A.R. and C.E. Tucker, *Encryption and the loss of patient data.* Journal of Policy Analysis and Management, 2011. **30**(3): p. 534-556.
14. *INCITS-499-Comments-due-2-28-2017 Next Generation Access Control - Functional Architecture (NGAC-FA).* 2016.
15. Moher, D., et al., *Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement.* International journal of surgery (London, England), 2010. **8**(5): p. 336-41.
16. Knobloch, K., U. Yoon, and P.M. Vogt, *Preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement and publication bias.* Journal of Cranio-Maxillofacial Surgery, 2011. **39**(2): p. 91-92.
17. OCLC, *WorldCat*. https://www.worldcat.org/.
18. *HIPAA Security Rule*. 2013: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
19. Hu, V.C., D.F. Ferraiolo, and D.R. Kuhn, *Assessment of Access Control Systems*. 2006, NIST: Gaithersburg, MD 20899-8930.
20. Samarati, P., et al., *Access control: Policies, models, and mechanisms.* Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2001. **2171 LNCS**: p. 137-196.
21. Landwehr, C.E., *Formal Models for Computer Security.* ACM Computing Surveys (CSUR), 1981. **13**(3): p. 247-278.
22. Jaehong, P., et al., *Towards usage control models: beyond traditional access control*. Symposium on Access Control Models and Technologies. 2002, ACM, 2 Penn Plaza, Suite 701, New York, NY 10121-0701, USA.
23. Ferraiolo, D.F., et al., *Policy Machine: Features, Architecture, and Specification*. 2015, NIST.
24. Androulaki, E., et al., *Hyperledger fabric: a distributed operating system for permissioned blockchains*, in *Proceedings of the Thirteenth EuroSys Conference*. 2018, Association for Computing Machinery: Porto, Portugal. p. Article 30.
25. IBM. *Hyperledger Fabric A Blockchain Platform for the Enterprise*. [cited 2021 5/21]; Available from: https://hyperledger-fabric.readthedocs.io/en/latest/.
26. Ferraiolo, D., V. Atluri, and S. Gavrila, *The Policy Machine: A novel architecture and framework for access control policy specification and enforcement.* Journal of Systems Architecture, 2011. **57**(4): p. 412-424.
27. Houtan, B., A.S. Hafid, and D. Makrakis, *A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare.* IEEE Access, 2020. **8**.