Heliyon 9 (2023) e18061

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

A blockchain-enabled sharing platform for personal health records

Yibin Dong *, Seong K. Mun, Yue Wang

Virginia Polytechnic Institute and State University, Arlington, VA, 22203, USA

ARTICLE INFO

Keywords:
Sharing platform
Personal health record
Blockchain
Patient consent
Security
Privacy
Trustfulness

ABSTRACT

Background: Longitudinal personal health record (PHR) provides a foundation for managing patients' health care, but we do not have such a system in the U.S. except for the patients in the Department of Veterans Affairs. Such a gap exists mainly in the rest of the U.S. by the fact that patients' electronic health records are scattered across multiple health care facilities and often not shared due to privacy, security, and business interests concerns from both patients and health care organizations. In addition, patients have ethical concerns related to consent. To patients, data security, privacy, and consent are based on trustfulness, rather than patients' engagement in ensuring only authorized people can view their PHRs with patient-managed granularity. Resolving these challenges is an important step in making longitudinal PHR useful for patient care.

Objective: This research aims to design and implement a blockchain-enabled sharing platform prototype for PHR with desired patient-controlled data security, privacy, and consent granularity.

Methods: Built upon our prior work of a blockchain-enabled access control (BAC) model, we design a blockchain-enabled sharing platform for PHR with patient-controlled security, privacy, and consent granularity. We further implement the construct by building a prototypical platform among a patient and two typical health care organizations. Health organizations that hold the patient's electronic health records can join the platform with trust based on the validation from the patient. The mutual trust can be established through a rigorous validation process by both the patient and the built-in Hyperledger Fabric blockchain consensus mechanism.

Results: We proposed a system trusted by patients and health care providers and constructed a Web-based PHR sharing platform with patient-controlled security, privacy, and consent granularity. We analyzed the system scalability in three aspects and showed millisecond range of performance when simultaneously changing access permissions on hundreds of PHRs. Consent, security and privacy of the model are ensured by the merits of the BAC model. We discovered the current blockchain model limits the system scalability due to using a non-graphical database. A new graphical database is suggested for future improvements.

Conclusions: In this research, we report a solution to electronically sharing and managing patients' electronic health records originating from multiple organizations, focusing on privacy, security, and granularity control of consent in the U.S. Specifically, the system protects data security and privacy, and provides auditability, scalability, distributedness, patient consent autonomy, and zero-trust capabilities. The prototypical instantiation of the designed model suggested the feasibility of combining emerging blockchain technology with next generation access control model to tackle a longstanding longitudinal PHR problem.

* Corresponding author.
E-mail address: yibin.dong@vt.edu (Y. Dong).

https://doi.org/10.1016/j.heliyon.2023.e18061
Received 14 June 2023; Received in revised form 30 June 2023; Accepted 5 July 2023
Available online 8 July 2023

1. Introduction

Longitudinal personal health record (PHR) is an individual-managed, "electronic, lifelong resource of health information needed by individuals to make health decisions" [1,2], to share information with providers, and to improve the quality of their own health care [3]. In the U.S., there are three types of PHR implementations: standalone, tethered, and untethered [4]. The standalone is managed by an individual (or patient), and not connected to any provider's electronic health record (EHR) system. The tethered is confined within a provider's EHR and co-managed through a partnership between the provider and the patient. The untethered is aggregated for a patient from multiple EHRs that the patient has encountered. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (the Privacy Rule) regulates how the health information enters the standalone [3]. Protected health information (PHI) in the tethered or the untethered is governed by the Privacy Rule [3]. Both EHR and PHR are aggregation of an individual's electronic health records from many health care organizations [5] that include "a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results" [6]. Differently, the former is managed by clinicians and staff in health care systems while the latter is controlled by an individual [5]. In addition, PHR can include patient-generated health data (PGHD) [7] from patients' personal health monitoring devices. Examples of this type of data are blood pressure tracking logs, dietary habits, or health related goals and exercise records. In this research, we focus on individual-managed longitudinal PHR (Fig. 1) [6] that consists of PHRs replicated from EHR systems that the patient has encountered, and the patient's own PGHD. It forms a holistic view of an individual's health records.

In the U.S., it is difficult to build a longitudinal PHR system. On one side, a health care provider (second party) is usually unwilling to share a patient's (first party) electronic health records with the third party, an individual or entity other than the patient and the health care provider that the patient has encountered. On the other side, privacy and security are the key concerns from both health care providers and patients. This presents a challenge to patients and providers who usually require patients' historical health record information for patient care.

Furthermore, patients have been raising ethical concerns related to consent and granular control of PHR in the past two decades [8]. Fairweather & Rogerson emphasized that "a patient's right to informed consent should be dominant" [8]. Under PHR sharing context, informed means prior to getting the consent from a patient to use or disclose the patient's PHR, the nature, benefits, and risks of use or disclosure of the health information should be communicated to the patient. Consent means the data subject (i.e. the patient) shall authorize the use or disclosure of data to an entity for its agreed purpose. In the U.S., under the Privacy Rule (45 C.F R. § 164.508.) [3], a patient's consent is needed when a covered entity [9,10] wants to disclose a patient's PHI to third parties. A patient should have direct control of their PHRs to ensure "nonmaleficence" of the data. Additionally, the patient should have informed granular choice to share the data [8]. Consent is desired to be specific. McGraw, D. et al. pointed out solely relying on consent provides weak protection on PHR because consent is too general and easy to obtain even with opt-in consent. They recommended each consent needs to be

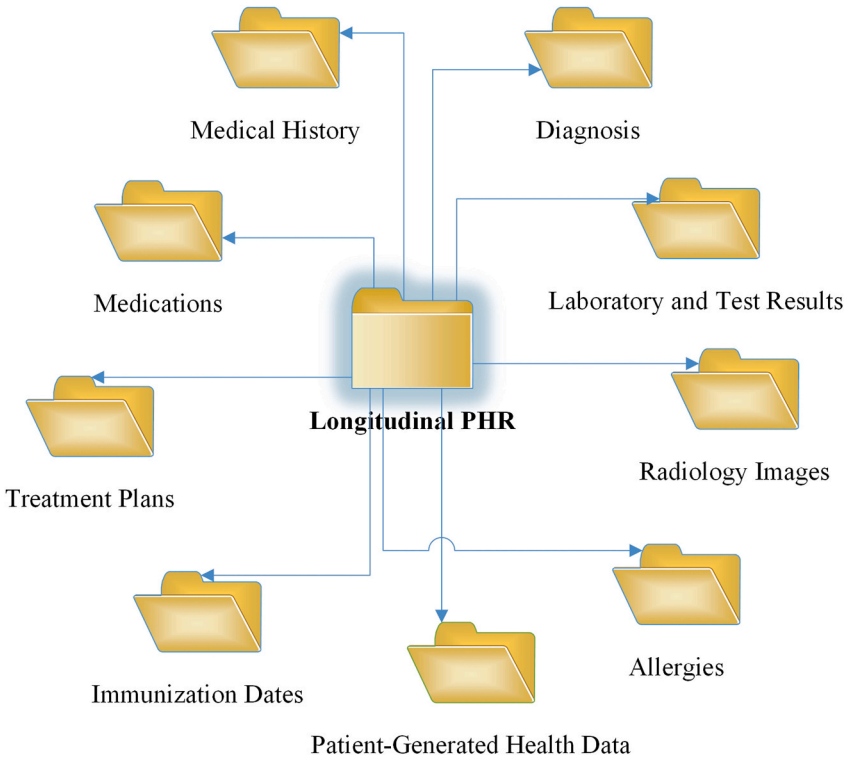

Fig. 1. Individual-managed longitudinal PHR.

specific to the purpose it is used for [11]. However, current consent practice in the U.S. is not that specific. They are either opt-out or opt-in [12–14] because getting proper informed consent from patients is a complicated [15] and sometimes very challenging task [16]. Shaw D. criticized that the opt-out consent system would fail because patients must affirmatively withdraw their consent otherwise consent was given by default. In case a patient wanted to stop sharing a specific record, the patient had to stop all content sharing. Patients desired to choose what specific patient record to share and with whom [17].

Dynamic consent has become an increasingly preferred method of consent choice for PHR sharing [12]. It is a bi-directional correspondence approach that patients can change the PHR sharing setting at any time with their preferences while the recipients of the shared data or research results of shared data can be informed to the patients [18,19]. Spencer, K. et al. concluded a patient-controlled digital dynamic consent system will "improve trust and engagement of electronic medical record research" [18]. In 2021, Thapa & Camtepe conducted a thorough review of legal, ethical, and clinical requirements around privacy, security, and trust for precision health, along with associated challenges and solutioning techniques [20]. They concluded that informed use of data is required, and patients shall have control of their health data. However, in dynamic consent, there is an open problem of "how to automate the consent and manage it efficiently in the interest of legislation, patient's autonomy, cost, and data analytics". Thapa & Camtepe suggested building "trust" to boost consent approvals [20].

Patients' understanding of (dynamic) consent, data security and privacy are based on the question of mutual trustfulness in both the organizations that provide health care service and the information technology service providers that offer the PHR platform. The patients who regard sharing data can strengthen privacy and security are inclined to consent and share PHR for health care [21]. Informed consent for PHR sharing for research is legitimate when patients fully understand what and how the data to be shared [22]. To study the patients' privacy and trust in VA, Damschroder, Laura J. et al. conducted a study by sampling 217 VA patients [23]. They found "patients' inclination to share their medical records for research" with VA researchers was associated positively with the trust in them. Most patients request for informed consent, security of sensitive information, clear communication, and consistent penalties of privacy violations. They found building trust during encounters was essential before sharing patients' data for research [23]. Therefore, patients want to be engaged and ensure only trusted people can view their PHRs. Solving this challenge of patient-controlled security, privacy, and consent granularity on PHR is an important step in making longitudinal PHR useful.

In our prior work, we have architected a novel blockchain-enabled access control (BAC) model, with individual-controlled granular access control update capability [2]. Contrasting to other previous works that provide PHR privacy protection using data encryption, we contributed to the body of knowledge via the perspective of preventing insider threats using access control policies based on the BAC model. Insider threat is a security risk mainly arises through the users inside or partners of an organization who hold legitimate decryption keys to the patient's data but misuse the permissions either intentionally or accidently. We argued that even with the best encryption methodology being applied on patients' PHR data, without a set of strong access control policies, the PHR data can still be leaked due to abused privileges inside of organizations [2]. In this research, we extended the model with use case studies in a simulated environment and tested key factors of patient-controlled security, privacy, and granular consent changes on PHR sharing. We designed and implemented a **b**lockchain-**e**nabled **s**haring pla**t**form (BEST) prototype for PHR facilitating a patient to securely share PHRs among the health care providers the patient encountered.

The rest of the paper is organized as follows: In the methods section, first, we list the design requirements. Second, we briefly describe the BAC and present the architecture of the BEST that consists of a patient and two model EHR organizations. Third, a high-level technical configuration of a prototypical security policy is illustrated. In the results section, key properties of the BEST are constructed to show fulfillment of the design requirements. A detailed Web-based implementation of the BEST is explained. System scalability is measured to show millisecond range of performance when simultaneously changing access permissions on hundreds of PHRs. In the discussions section, key features of the BEST are elaborated. The cost of PHR data management is examined and the limitations of the design are identified. We wrap up the paper with a conclusions section.

2. Methods

This section states the methodologies used in the BEST model. We start with a design requirements analysis of a patient trustful secure PHR sharing platform. Then we briefly describe BAC and explain the rationale for choosing blockchain technology as part of the design. Next, we show the BEST for PHR model and architecture along with an example of access control policy configuration.

2.1. A patient trustful secure PHR sharing platform requirements

All the requirements analyzed in our prior work [24] (Appendix A) are applicable to a patient trustful secure PHR sharing platform. They include PHR security, privacy, access auditability, scalability, distributedness, interoperability and integration. There are two additional requirements to meet that are specific to consent and sharing.

A) **Patient's Consent Autonomy**: Patient consent autonomy means the patients who have decision-making capacity shall have granular control of the consent of their medical information when sharing the information with third parties [18,25]. In the U. S., consent is not freely given. Instead, it is an opt-in or opt-out choice. To share the patients' PHRs to third parties for research or health care, patients desire to have granular control of the consent of sharing [18].

B) **PHR Sharing Zero-trust**: Zero-trust security model is a trend in enterprise-level information security and privacy protection [26]. The main idea of the model is authentication and authorization are verified each time PHR information is being accessed. For example, a hospital is trusted by a patient, and all the patient's non-mental health psychotherapy notes information can be

viewed by all doctors in the same hospital. However, the patient's mental health psychotherapy notes can be only viewed by a designated authorized doctor, but not other doctors in the same hospital. Accessing the patient's health records is never trusted by default and always validated in real-time [26].

2.2. BAC

PHR sharing privacy and security are complex problems. Encryption is an intuitive way of guarding PHR privacy and confidentiality and being adopted by many pioneering works of PHR protection [27–34]. However, without a set of access control policies, applying encryption alone on PHR data cannot guarantee patient data security and privacy due to insider threats [2,27–34]. The policies pertain to privacy, confidentiality, integrity, availability, and competency [35]. PHR access control policies are non-static [35] because changes in government regulations and laws require the policies to be updated accordingly to reflect the compliance to regulatory rules. The policies are implemented through access control models, which are formal representation of the policies and their implementation reinforcement mechanisms on the systems being designed [35,36].

A secure PHR must possess the following properties [2,36,37]:

- The access control model is secure w.r.t. meeting the risk and compliance requirements of an organization;
- The model is correctly implemented through access control mechanisms;
- The system that adopts the model is correctly used by users.

To find an access control model that can meet the need, we compared traditional access control models with next generation access control (NGAC) models. Traditional access control models, such as role-based access control (RBAC), are established in a closed, centrally controlled, and server-oriented access control environment, in which users are well-known [38]. NGAC models are based on open access control surroundings where users can be either centrally known or unknown [35]. Since the users of PHR can be centrally known or unknown, NGAC is a better choice. In NGAC, all users share a set of access control policies residing in a central database [35]. This caused a gap with applications to distributed systems like PHR because it can suffer a race condition when multiple remote users try to read or write a central access control policy database at the same time. The policy database needs to be accessed by a set of database operations in sequence. However, if there is a processing delay, a later access request might get a copy of the policy of an earlier state. This is an undesired result in PHR access control. To fill this gap, we adopted permissioned blockchain Hyperledger Fabric (HF) to solve the NGAC racing condition problem [2]. The HF offers concurrency control contributed from HF consensus [39] to ensure the policy database is accessed in the sequence of chronological order of access requests. We offered BAC which is an integration of NGAC with HF.

In BAC model (Fig. 2) [2], resources (policy enhancement point (PEP), policy decision point (PDP), event processing point (EPP), resource access point (RAP)) [40] forcing the access control policies are locally distributed [2]. Any access requests to protected PHR

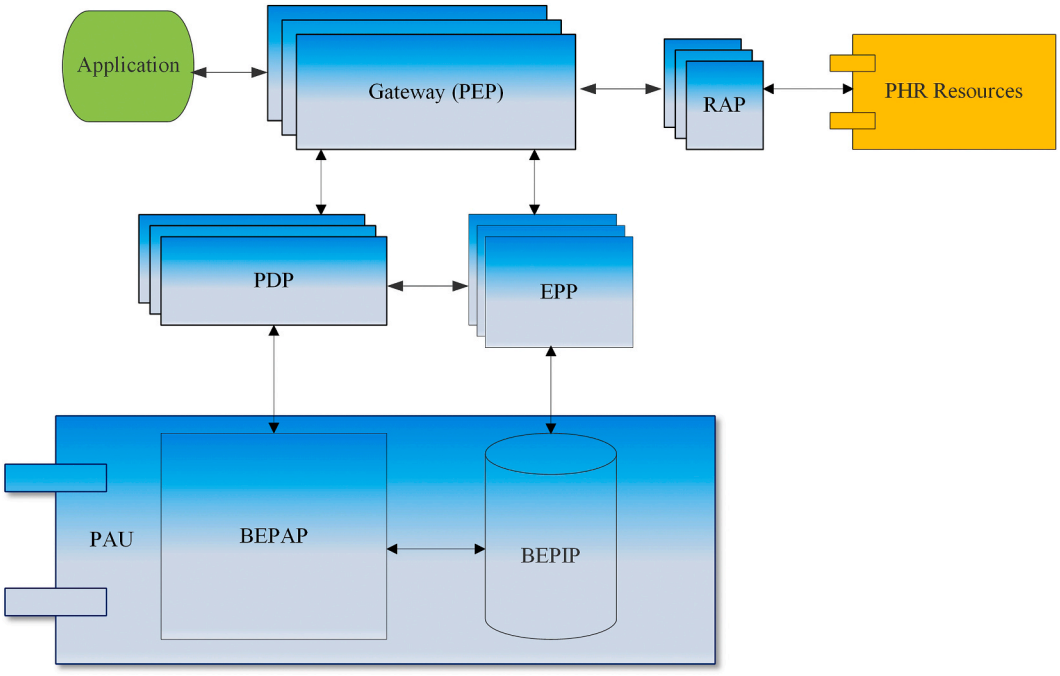

Fig. 2. BAC model.

resources or inquiries to access control policies are managed by the PEP, which can be viewed as a gateway. The PDP acts as a decision maker to the access requests sent through the PEP. The EPP is crucial when an event response is specified in a policy. An example of an event could be a physician trying to read a restricted mental health psychotherapy note. A set of automated actions defined in a policy will be triggered to grant or deny the read attempt operation. The RAP manages the access to protected PHR resources exclusively through the PEP. Blockchain-enabled resources (blockchain-enabled policy administration point (BEPAP) and blockchain-enabled policy information point (BEPIP)) are decentralized and form a BAC policy administration unit (PAU) [2]. Identical BAC policies are shared by the applications accessing the policy database BEPIP [2].

2.3. The BEST for PHR

The BEST is built upon the BAC authorization model (Fig. 3) [2] to meet additional requirements of PHR consent and sharing of patients' authorized PHRs, and is unique and personalized to the PHR data subject. The personalization emphasized is the patient-controlled security, privacy, and granular consent via a set of unified access-control policies using blockchain technology. From an application interface, a user is securely authenticated using a digital certificate, which is compliant with the X.509 cryptographical public key infrastructure (PKI) standard [41] that defines the format of the digital certificate. The user can be the patient or EHR providers. The authorization is managed through BAC. Once access permissions are verified, the user can access the shared PHR. The BEST provides a Fast Healthcare Interoperability Resources (FHIR) [42] interface which is employed to retrieve the patient's PHR information that is in the EHRs the patient has encountered.

The BEST for PHR architecture is shown in Fig. 4. To demonstrate the design, we show a 3-organization use case. We built a simulated EHR environment using open source VistA [43] and simulated PHR [44]. VA has been using VistA in the past 30 years to operate over 150 hospitals [43]. VistA_EHR_A and VistA_EHR_B represent two different EHR organizations that a patient has encountered. In this setting, the patient is considered as one organization and will consent and share the PHR (triangle shape) generated from VistA_EHR_A with VistA_EHR_B. There are two secure communication channels in system. A BAC policy secure channel is used to share the permission information about the patient's shared PHR. A BEST data secure channel is established to share data. Only selected data that is consented by the patient are shared on the data secure channel. The PHR will be securely stored in off-chain encrypted databases managed by patients or providers. The shared data also contains an FHIR application programming interface (API) reference to the PHR located either in the sharing organization's choice of secure storage or patient's longitudinal PHR storage.

In order to share PHR generated from VistA_EHR_A with VistA_EHR_B, both EHR organizations need to join the BEST as trusted members. The "join" is realized via an onboarding (or provisioning) process in which the applicant organization, such as VistA_EHR_A, is assigned with a secure and unique identity. The health care provider adds the patient's PHR information generated during the encounter to the patient's longitudinal PHR. The health care provider is responsible for the integrity of the data since this is the source of the patient's PHR. The patient is a consumer and data subject of this part of PHR. The patient can control the granular permission to share this data with third parties. The trust between the patient and the health care provider is built during the initial encounter. The

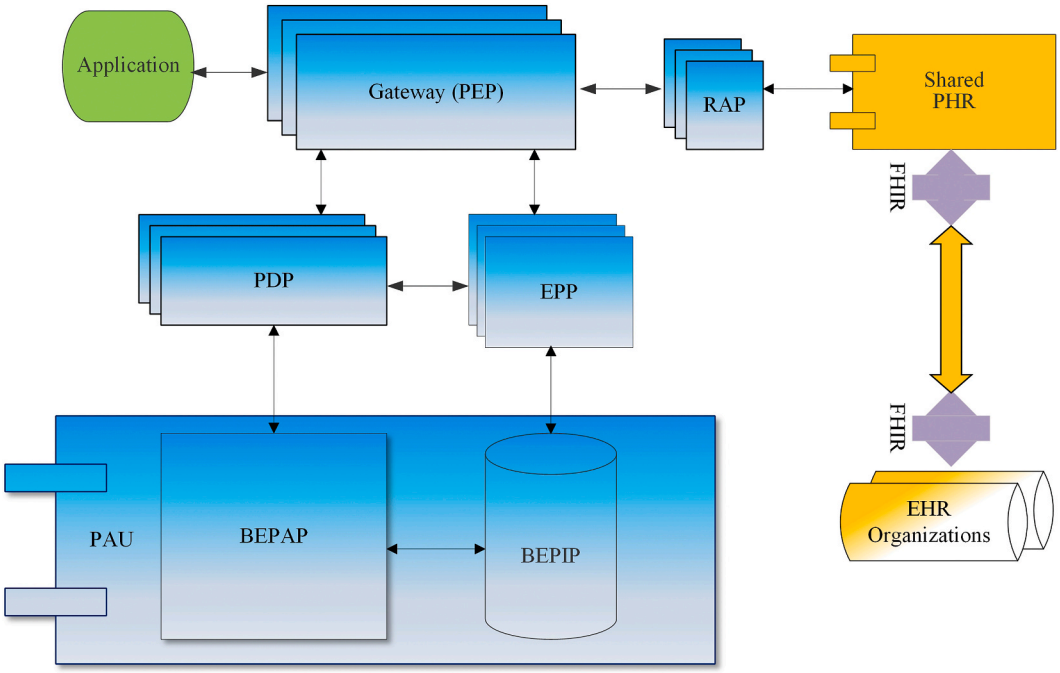

Fig. 3. BAC authorization for the BEST.

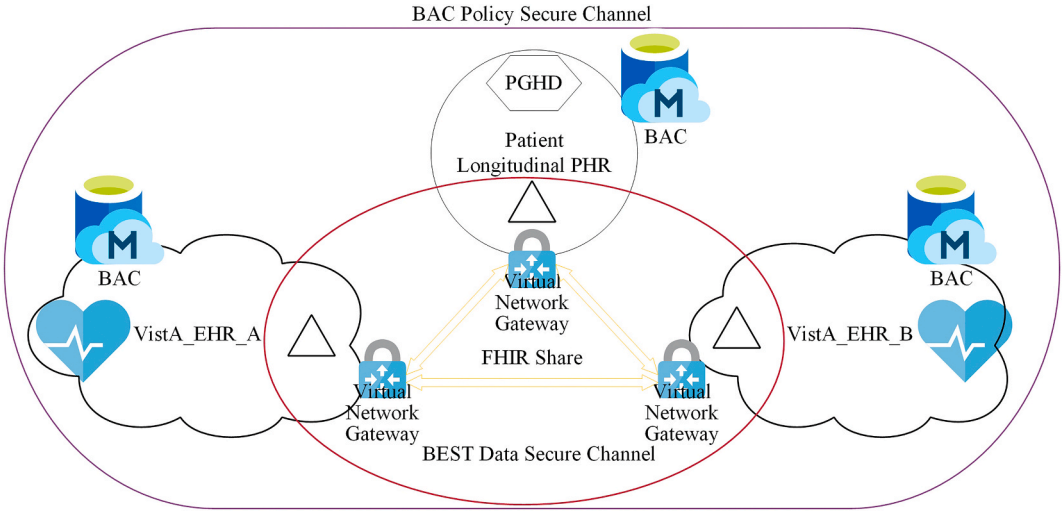

Fig. 4. The BEST for PHR architecture.

onboarding process for one EHR (e.g. EHR_A) is illustrated via a sequence diagram in Fig. 5. The patient visits a physician in EHR_A. The physician creates the patient's PHR in EHR_A. The patient then sends a request to the BEST administrator to add EHR_A as a trusted member to the BAC policy secure channel. The administrator creates a secure identity for EHR_A on the BEST. The administrator adds EHR_A to the BAC secure policy channel and sends notifications to the patient and EHR_A physicians. Afterwards, the patient sends a request to the administrator to add the PHRs generated in EHR_A to the patient's longitudinal PHR. The administrator creates a BEST data secure channel among the patient and EHR_A. The administrator then sends a request to EHR_A to add the patient's PHR to longitudinal PHR. The physician logs in to the BEST with the secure identity and adds the patient's PHR to longitudinal PHR through an API integration process. The patient validates the newly added PHR data on the longitudinal PHR.

Once both VistA_EHR_A with VistA_EHR_B are onboarded, the patient can take the request from EHR_B to share the PHR generated during encounter of EHR_A as illustrated in Fig. 6.

A physician in EHR_B sends a request to the patient to read some PHRs generated from EHR_A. The patient reviews the request, provides granular consent of the sharing to EHR_B and updates the shared BAC policy. The patient sends a request to the BEST administrator to share the consented PHR to EHR_B. The administrator creates a transient data secure channel among the patient, EHR_A, and EHR_B and informs the patient of the readiness of data sharing. The transient data secure channel only exists for the specified sharing. The patient notifies the physician in EHR_B about the approved sharing request. The physician in EHR_B logs in to the BEST, lists the PHRs shared with EHR_B, and retrieves the desired PHR shared from EHR_A.

In the BEST, the PHR that replicated from a health care provider's PHR is stored in the patient's longitudinal PHR as read only, which is required and regulated by the Privacy Rule. The patient can request to add supplementary information, but any changes need to be completed by the provider. The patient cannot delete this type of PHR. The patient has the control of what PHR to be shared with whom, based on a request from the party that intends to use the PHR information. The BEST for PHR reference architecture is shown in Fig. 7.

2.4. Technical configuration of the access control policy

In the BEST, PHR access permissions are managed through assignments of attributes that possess common properties and characteristics of users or objects [45]. Examples of user characteristics are functions of specific roles such as doctor, nurse, or researcher. Examples of object characteristics are data repository location (e.g. VistA_EHR_A), or resource type (e.g. PHR). The BAC policy elements, assignments, and access decision making processes are defined by set and binary relations (Appendix B) [24]. To illustrate the patient-controlled authorization and trust established among the patient and two EHR organizations, we provided an example of the BEST technical configuration of BAC access control policy in Appendix B. Figure B1.

3. Results

In this section, we firstly show how the BEST solution meets the design requirements. Afterwards, we explain details of the BEST implementation with a Web-based application. Patients are provided with a personalized Web portal to manage security, privacy, and consent of PHRs. A lighter version of the Web portal is offered to providers to manage accessing the patients' shared PHR. The BEST system scalability analysis will follow.

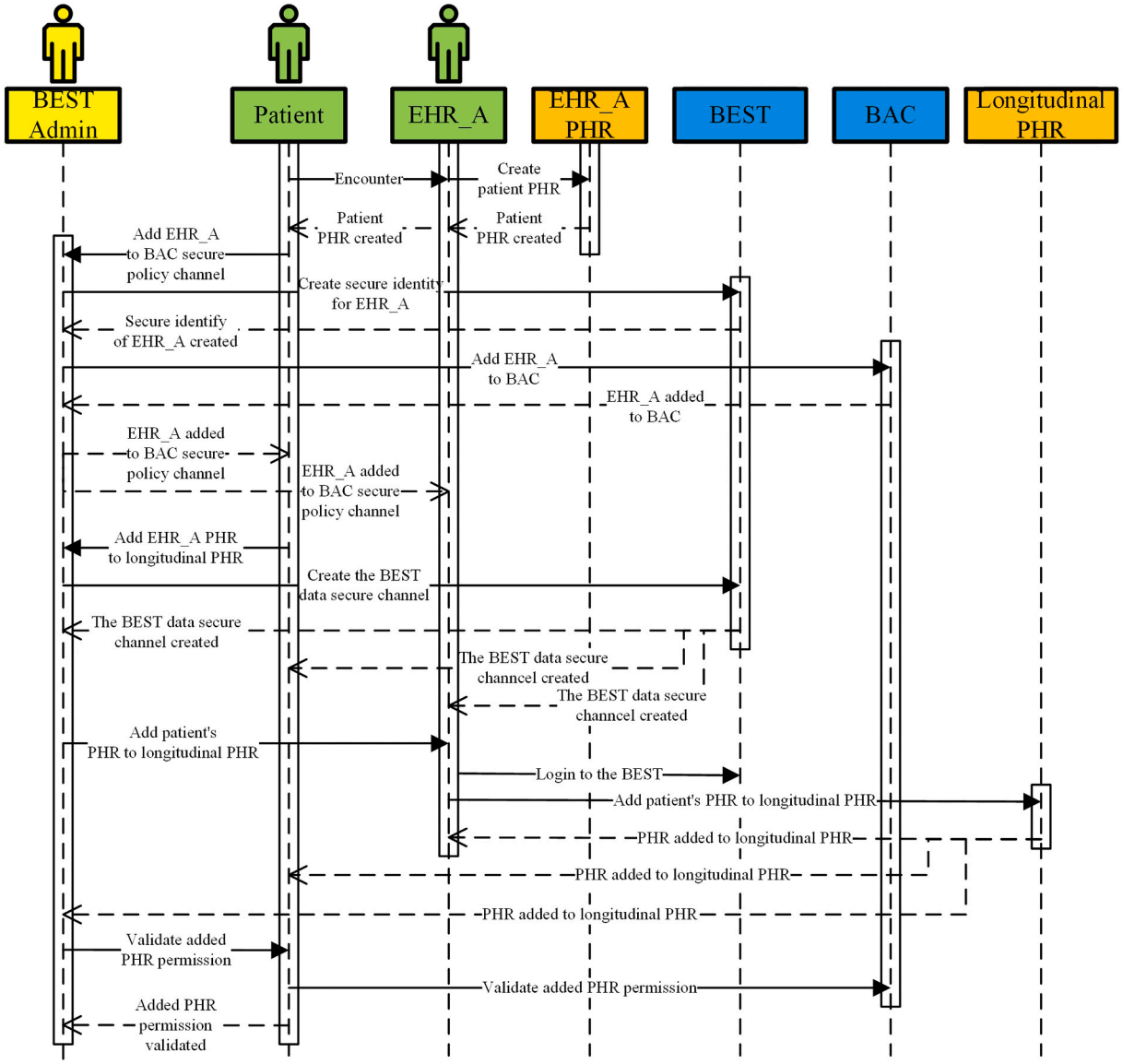

Fig. 5. Onboard one EHR to the BEST sequence diagram.

3.1. System design requirements fulfillment

In the BEST model, HF blockchain, NGAC, and FHIR jointly present properties that fulfill the design requirements (Table 1 [24]).

Security and Privacy: PHR security includes confidentiality, integrity, and availability [46]. PHR privacy is about hiding information from unauthorized people or processes. Within the scope of the Privacy Rule [47] and the HIPAA Security Rule [48], PHR privacy is related to the collection, storage, usage, and disclosure of personal health information [49,50]. The Privacy Rule guides the justifications of personal health information collection, ownerships of the acquired health information, storage conditions of collected health information, usage specificity, and disclosure prohibitions. Under the U.S. Office of the National Coordinator for Health IT (ONC) Cures Act Final Rule and the Centers for Medicare & Medicaid Services (CMS) Interoperability and Patient Access Final Rule, use or disclosure of patients' health information either requires authorization from patients, who directly control the privacy of their health information, or is obligated to local, state, or federal laws [51,52].

PHR is protected by BAC policies to ensure security and privacy. The policies disallow use and disclosure of PHR to unauthorized parties [2] which fulfills the *confidentiality and privacy* requirements. The policies prevent the PHR from being altered or destroyed in an unauthorized manner [2,48] which ensure the *integrity* (including accountability) of PHR. Data integrity is further protected by the immutability and tamper resistance properties of HF blockchain. Any changes to the PHR are timestamped. The policies guarantee the PHR is accessible and useable on demand by an authorized person [2,48] that fulfills the *availability* requirement [48]. The computer

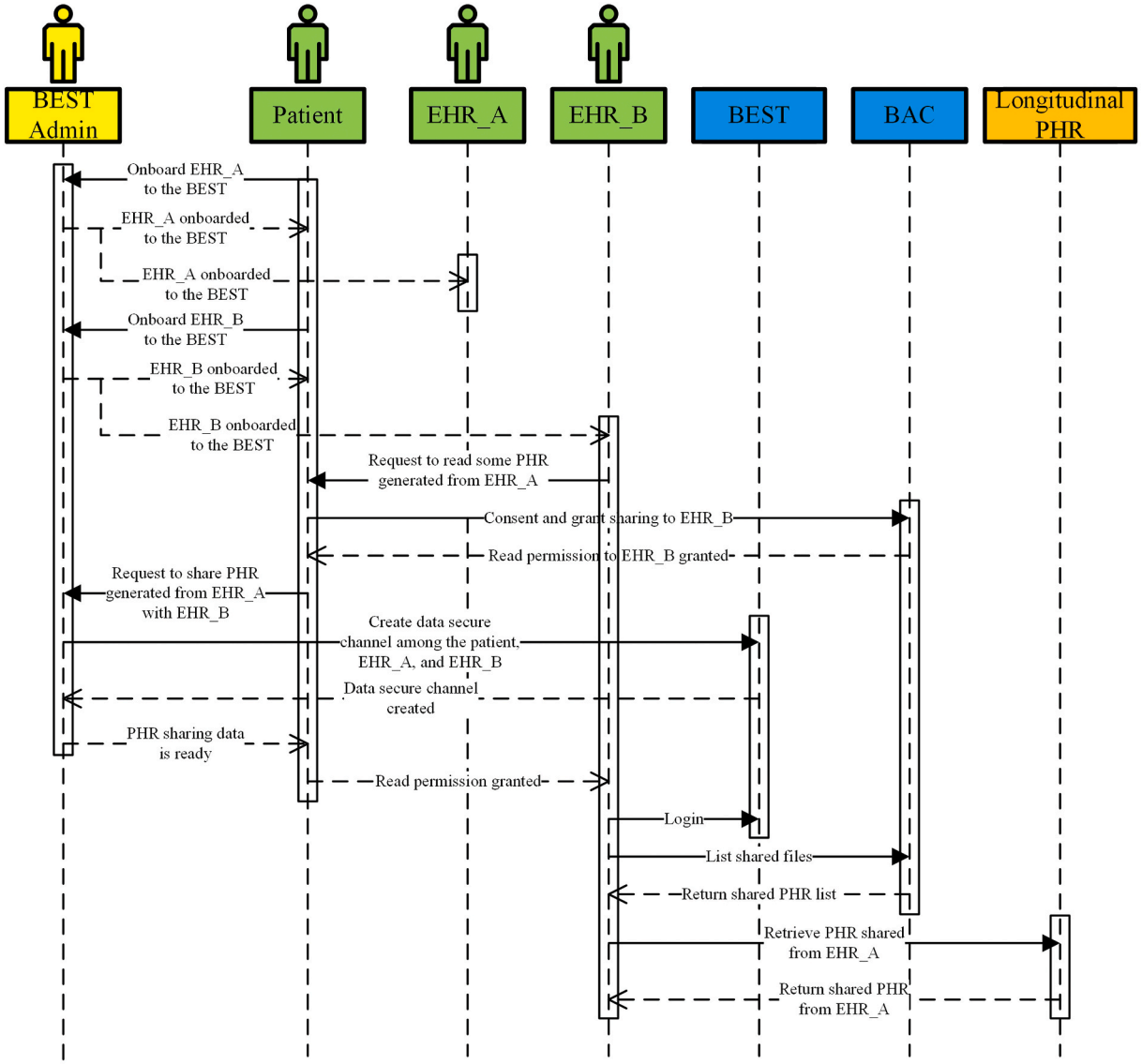

Fig. 6. Share EHR_A PHR with EHR_B sequence diagram.

applications are configured to access the BEST through user accounts or profiles that contain authorization permissions associated with BAC access control policies. The authentication to the BEST is through a secure public key infrastructure X.509 digital certificate that guarantees login security. The encryption of blockchain is managed through the digital certificate that is assigned to the patient by the platform administrator. The platform administrator also provides a key recovery mechanism, in case the patient lost the secure certificate, to ensure the availability of the secure key [24].

Access Auditability: The HF audit logs keep the history of changes to the BEST. It inherits the HF blockchain non-repudiable property.

Scalability: The designed model is enterprise scalable because both NGAC and HF are enterprise scalable [2,40,53].

Distributedness: The unified access control policies are managed through the BAC. The policies reinforcing units (PEP, PDP, RAP, and EPP) are distributed to fulfill the PHR distributesness requirement. The PHRs are distributed in the EHR organizations that the patient has encountered.

Interoperability and Integration: PGHD from smart or wearable personal devices are integrated to the patient's longitudinal PHR. A FHIR interface is provided in the BEST to interoperate with other EHRs.

Patient's Consent Autonomy: Patients have full control of the permissions of their own records. The access control information is stored in the BEPIP database, which is distributed yet decentralized among trusted parties on the secure HF blockchain network. A patient can give very granular consent to use their PHR by trusted providers, which will improve the trustfulness between patients and providers. The trust is built during the initial encounter between the patient and the provider. Through interaction with the health care

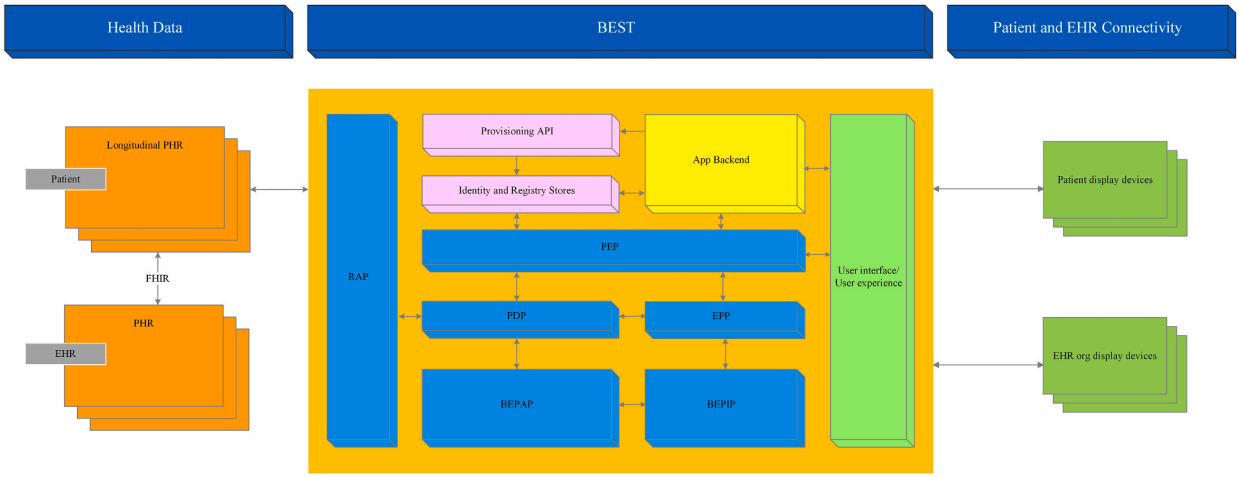

Fig. 7. The BEST for PHR reference architecture.

Table 1
Patient trustful secure PHR sharing platform requirements fulfillment.

Requirements	NGAC	HF Blockchain	FHIR
Security (Confidentiality, Integrity, and Availability)	X	X	
Privacy	X	X	
Access Auditability		X	
Scalability	X	X	
Distributedness	X	X	
Interoperability and Integration			X
Patient Consent Autonomy	X	X	
Sharing Zero-trust	X	X	

provider, the patient can learn how secure the PHR is handled by the provider.

LPHR Sharing Zero-trust: Access requests to the BEST are always validated by the BAC policy decision maker before granting or denying access permissions.

3.2. System implementation

We built a prototypical environment for simulating a three-organization BEST, in which the patient, VistA_EHR_A, and VistA_EHR_B are the representative organizations. After establishing a playground (Appendix C.1. The BEST simulation environment) [24], the BEST was constructed with steps as below:

1. Start a HF network with two organizations: The patient (Org1) and VistA_EHR_A (Org2).
2. Create a BAC policy secure channel.
3. Add the third organization VistA_EHR_B (Org3) to the policy secure channel. This step is to demonstrate the capability of adding additional organizations to the secure channel.
4. Deploy policy smart contracts (or chaincode) to the policy secure channel on all three organizations. The policy smart contracts handle the policy information transaction such as query or update policy information, and granular consent.
5. Register secure identities to each of the organizations. The owner's identity is registered to Org1. The EHRA identity is registered to Org2, and the EHRB identity is registered to Org3.
6. Initialize the policy database (BEPIP) with PHR permissions using the owner's identity. The permissions are explained in the "Appendix C.2. BAC permission tree of three organizations" section [24].

At this point, the policy database is populated with access control permissions information. Our next step is to build a data sharing network. For simplicity, we will use the same HF blockchain network where the policy information resides. In real world applications, the data sharing can be on a different HF blockchain network. The data sharing network is constructed as follows:

1. Create a BEST data secure channel with three organizations: The patient (Org1), VistA_EHR_A (Org2), and VistA_EHR_B (Org3).
2. Deploy data smart contracts to the data secure channel on all three organizations. The data smart contracts handle the PHR secure sharing transactions, such as query shared PHRs.

3. Use the authentication secure certificate of each corresponding organization to populate the BEST with some sample data.

We built a Web-based application portal using open source programming language Go [54] that supports multi-cores with built-in concurrency computing capabilities to further fulfill the PHR scalability requirement. We have provided two different management views, one for patients and the other for EHR doctors. In the BEST patient management view (Appendix D), a patient can perform permission management on PHRs and view details of PHRs. The patient can assign a health record to the patient's own PHR attribute or provider's PHR attribute. Similarly, a health record can be removed from the patient's own PHR attribute or provider's PHR attribute. The patient can share PHRs from one provider with another or share from the patient's own PHR. Sharing permissions revocation can be done in the same way. In the EHR doctors' management view (Appendix E), a doctor can perform limited permission management on patients' PHRs and view details of patients' shared PHRs. A doctor can add doctors in the same EHR organization or remove users (doctors). All permission changes are validated against the shared BAC policies. In both management views, we implemented automated security and privacy controls via event response rules (Appendix F). An obligation (event response) is initiated by a user triggering an event response corresponding to an event pattern. When a process executes an operation that can impact the access control of a PHR, one or more obligations might be triggered. The obligations are required to be fulfilled in the order they were generated before the next event response being generated. The coordination of the ordered event responses is handled by BAC.

3.3. System scalability evaluation

The scalability of the BEST can be evaluated in three aspects, in which all are related to the scalability of underlying BAC scalability performance: (1) Inner-Patient: The number of PHRs' permissions one patient can simultaneously grant or change, and the cost of time to make the change. (2) Patient-to-EHR: The number of EHRs one patient can share the permission with. (3) EHR-to-Patient: The number of patients one EHR organization can onboard.

For Inner-Patient, we conducted a simulation test of assigning new patient PHRs to the patient using the PHR record IDs. Firstly, we turned the timing on and loaded the current BEST permission tree graph from the HF blockchain into the computer memory. Secondly, we looped through a list of simulated PHR record IDs and updated the permission tree graph. Lastly, we updated the HF with the newly modified permission graph and turned the timing off. The total cost of time T_{total} is shown as follows:

$$T_{total} = T_{rHF} + T_{uGraph} + T_{wHF}$$

Where T_{rHF} is the time used to retrieve the BEST permission graph tree from HF blockchain, T_{uGraph} is the time spent to update the permission graph tree in the computer memory, and T_{wHF} is the cost of time to update the BEST permission graph on HF blockchain.

The permission tree was initialized with 6 patient records. One hundred patient records were added to the permission tree each time. We repeated the process and the program was stopped at inserting the 791th patient record due to a Linux command-line bound limitation in the current design. The time consumption is summarized in Table 2. In this experiment, the cost of time to insert 100 patient records is ranging from 123 ms (ms) to 236 ms (Fig. 8).

We further conducted a load testing of inserting 784 patient records into the permission tree. The testing was repeated 1000 times. Averaging over 1000 iterations (Fig. 9), the mean value is $\overline{T_{total}} = 187.549271\ ms$ with a standard deviation of

$$\delta = 53.4497849\ \ ms$$

The above testing was executed in an environment where all organizations are on the same virtual machine. Therefore, the performance is almost instant at millisecond scale. In a real-world scenario, organizations on the HF secure channel are likely geographically scattered. T_{rHF} and T_{uGraph} are still calculated locally, however, T_{wHF} can vary due to processing delay if there is a communication latency or error when writing data to the HF off-chain database.

For Patient-to-EHR, the number of organizations the patient can share permission with is theoretically unlimited. However, it is bounded by the limit of the software and hardware used to implement the system. For the current design, it will hit the same Linux command-line bound limitation on the construction of the permission tree. Also, it will be restricted by the maximum number of EHR organizations that can join the same HF blockchain channel.

For EHR-to-Patient, the maximum number of patients one EHR organization can onboard is also theoretically unlimited. The EHR organization and the patient form a secure HF channel, which will be established on a small scale of the HF blockchain network. The

Table 2
Time consumption to insert patient records to permission tree.

The number of patient records inserted	The number of patient records on HF blockchain	T_{rHF} (ms)	T_{uGraph} (ms)	T_{wHF} (ms)	T_{total} (ms)
100	106	71.419995	0.106323	65.11438	136.640698
100	206	74.081626	0.084857	71.908411	146.074894
100	306	61.198432	0.053707	61.853269	123.105408
100	406	76.109884	0.106680	116.906602	193.123166
100	506	86.403810	0.098089	62.156150	148.658049
100	606	59.150527	2.228658	76.420628	137.799813
100	706	77.629765	0.076686	83.848741	161.555192
84	790	91.456703	0.110604	144.965081	236.532388

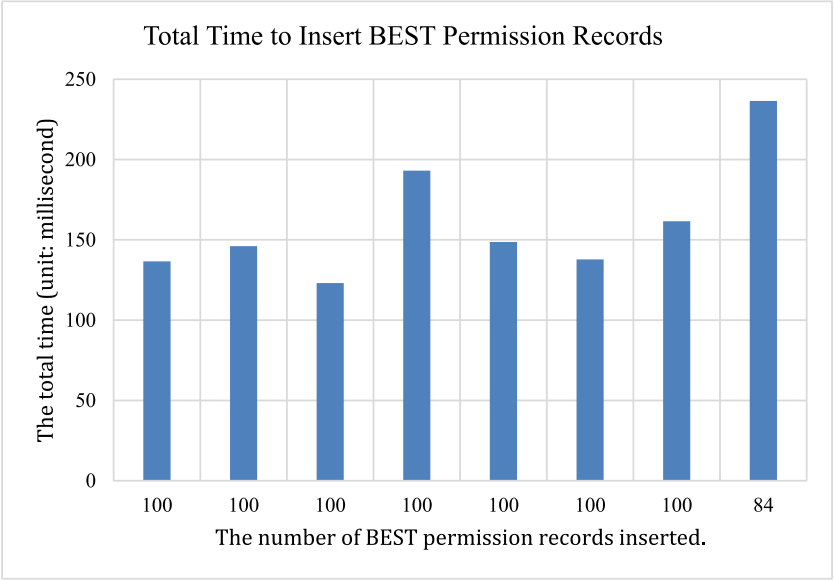

Fig. 8. Total time to insert BEST permission records.

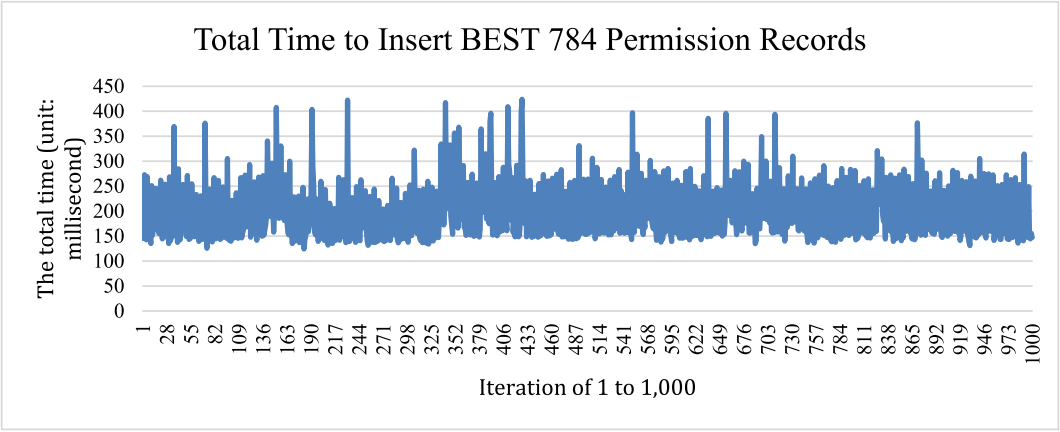

Fig. 9. Total time to insert BEST 784 permission records.

limitation is based on the hardware and software capacity each EHR organization uses to build the HF network.

4. Discussions

4.1. The BEST security privacy and consent management

In the U.S., when patients are engaged with a clinician or health care team, an individual's PHR information is expected to be flowing freely in the health care systems the individual encounters. There have been various challenges such as interoperability [55, 56], security, and privacy concerns [48,57,58]. In this research, we focus on security and privacy concerns. PHR sharing resistance is usually caused by low trust between patients and providers. Patients are willing to share their PHR information via informed consent if the trust has been established. Trust is a representation of PHR security and privacy. The current consent in the U.S. health care system is either opt-in or opt-out. Patients want to granularly manage the consent on their own PHR, so they know who has access to what information of their PHR at what time. We offered the BEST, a PHR sharing solution focusing on preventing insider threats with patient-controlled security, privacy, and consent granularity. Threat prevention is achieved via BAC. The consent is realized through access control policy assignments that are stored in the blockchain-enabled access control policy database.

The permissioned blockchain HF technology fits the PHR sharing environment that EHR organizations and the patient have built a permissible trust relationship during initial encounters. Blockchain's unique security and privacy protection properties established a playground for this setting. Next generation access control policies enhanced informed consent capability. When combining HF with

NGAC to build BAC, the offered product BEST meets the requirements naturally. The BEST is personalized to the patient, so each BEST has unique PHRs information and the access control is managed by the patient. The off-chain storage of BAC and the BEST enhance data security. EHR organizations have freedom of choice of data encryption methods. Our Web-based application implementation demonstrated its capability of security and privacy protection as well as granular patient-controlled informed consent. Each organization is required to login through a secure authentication method. Rather than focusing on identity management (decentralized authentication) [59], this research concentrates on decentralized authorization. The automated event responses capability offered by the BEST is a key differentiator from other solutions using blockchain-supported attribute-based encryption [60].

4.2. The cost of data management

In the design, we assumed all parties are willing to use PHR. The real-world adoption of the solution requires all key players, such as patients and EHR organizations, to establish a mutual agreement to share PHR information. There are few challenges to each of the parties. Patients need to easily access the BEST system that stores their PHR information. Most patients probably do not have capabilities to establish such a system due to time, technical skills, or monetary constraints. Therefore, for patients to be engaged in, a third-party BEST-*as*-a-Service (BESTaaS) can be considered to provide technical platform and management service to individuals. Patients can pay a subscription fee to use the BESTaaS. The platform administrators manage the infrastructure and software stack that support the BESTaaS, which include but are not limited to authentication certificates or keys, blockchain secure channels, blockchain smart contracts, EHR organizations onboarding, and Web portals. For patients to use such a system, initial user training is also an inseparable step to reduce the barrier of engagement. For EHR organizations, it is required that their IT infrastructure can support HF blockchain hosting the BEST software and keep high availability of the service. They can either maintain their own BEST infrastructure or use a BESTaaS service. Each patient's profile and the BEST can reside on a micro-container. The EHR organizations need a management console to administer all patients' profiles and micro-containers. These micro-containers have FHIR interfaces to the EHRs they manage. EHR organizations also want to ensure sustainability of the blockchain, which must coexist with the EHR systems employed.

4.3. Limitations

There are several limitations of this design. Firstly, this study is confined within the U.S. So, it might not necessarily be generalizable in another country. For example, PHI is an American terminology. In the European Union, health data is a special category of data under General Data Protection Regulation (GDPR) recital 35 [61]. More analysis is recommended to include GDPR specific requirements into the BEST design.

Secondly, even though a patient has full granular control of sharing the PHRs, there are challenges impacting the ability of sharing decisions. In most situations, a patient receives a request from one health care provider to get a copy of the PHR encountered in another health care provider. Personal patient factors, such as education, health status, age, contribute to the challenges of making an informed decision. Our method is restricted to patients with appropriate decision-making capacity. The patient may or may not have enough knowledge to wisely share the health information granularly. A comprehensive discussion might be required for patients to understand the PHR information they are sharing so adequate decisions can be made. For health care providers, it will be beneficial to explain to a patient what data needs to be shared and the intended use. A patient may also have difficulty using the BEST that is related to Internet and computer experience or capability of managing the authentication certificate. We suggest providing a BESTaaS to manage the secure certificate for the patient and offer technical training to patients. For young children or sick people who are either mentally or physically unable to make proper decisions, informed consent by the patient is difficult to obtain [16]. Consequently, these patients might not be able to provide granular control on their PHRs. They need to delegate the authority to their guardians or someone legally they can trust.

Thirdly, trust in PHR sharing is a social-technical or behavioral concept. Spencer, K. et al. confirmed a patient-controlled consent system will "improve trust" [18]. We technically prove the feasibility of building the BEST to enable patient-controlled consent, security, and privacy. However, to prove the translation from technical feasibility of trust to social-technical or behavioral feasibility of trust, more research is needed to use real world PHR data. Due to time and financial constraints, we plan to conduct the research in the future.

Fourthly, in the BEST each EHR organization is expected to handle transactions of hundreds of patients' PHRs. The current implementation inherited CouchDB, a key-value store for keeping each patient's BAC permissions graph. Since the permissions graph is updated when there is a permission change, the whole graph needs to be loaded into memory via a command line. In our system scalability test, the updated permission graph hit a Linux command-line size limit of 140 kB (143,689 bytes), which is equivalent to simultaneously adding 784 patient records' permissions to an organization for one patient. This problem needs to be solved when the complexity of one patient's permissions graph is high. In the future, we plan to address this issue by replacing the backend CouchDB with a graphical database such as Neo4j [62] to store BAC permissions graph.

Furthermore, in this implementation, we used HF version 2.3.2 with Raft protocol based crash fault tolerant (CFT) service [39] in HF orderer. A subset of the organizations joins the BAC or BEST secure channel forming the blockchain ordering service. The Raft ordering service employs a leader-follower model in which the leader is important to remain reachable at any time when blockchain transactions are in progress. In case there is a communication error to the leader node, a re-election mechanism is activated to promote a new leader from the surviving reachable nodes. The communication error can be caused by a processing delay or network indeterminate interruption. Each node in an organization might have orderer roles in both BAC and BEST secure channels. The undesired leader re-election can introduce communication overhead and extra load to the HF network. Therefore, it is recommended to construct

BAC or BEST channel ordering service with less than 10 organizations to gain optimal performance, and each orderer joins no more than 50 secure channels [39].

Moreover, our software code integrated the National Institute of Standards and Technology Policy Machine, HF blockchain module, with the BEST smart contracts. The current version is highly customized to show a feasible and working orchestration in a simulated environment. We plan to optimize the software to be more concise and modular. Also, we have reserved a FHIR API configuration socket for future work using real EHR organizations' FHIR servers.

Lastly, we only demonstrated the event processing capability of the BEST of an obligation (event response). There is another type of capability of prohibition which we plan to implement. The prohibition is especially useful in data loss prevention. For example, when one user is reading a medical record, we can apply a prohibition access control policy to prevent the same user process from writing to any other medical records so to prevent the patient data being leaked. The prohibition can be on process level or user level or both.

5. Conclusions

In this research, we expanded our work of BAC and built a novel patient-trustful blockchain-enabled sharing platform for PHRs. The patient is anchored at the center of controlling the consent and sharing their PHRs to third parties. EHRs that hold the patient's PHRs join the BEST with trust which is validated by the patient. The mutual trust is established on a rigorous zero-trust validation process by the patient and built-in HF consensus offered by the BEST. The security, privacy, scalability, and distributedness of the BEST are governed by BAC policies. The auditability is insured by HF blockchain technology. The interoperability and integration are supported by FHIR. While other research focusing on secure authentication or encryption, our solution reaches deeper into granular patient-controlled authorization with automated event response and prohibition capabilities to prevent insider threats. We demonstrated its feasibility by having implemented the prototypical design and applied to a use case of patient-controlled PHR sharing among two model EHR organizations and the patient. We evaluated the limitations of the current design and implementation with improvement recommendations.

6. Code availability

All software used in building the simulation platform are open source and will be available upon request from GitHub repository at https://github.com/ydong01/bengac and https://github.com/ydong01/asset-transfer-private-data. Please send GitHub ID to the corresponding author to get access to the source code.

Author contribution statement

Yibin Dong: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed materials, analysis tools and data; Wrote the paper.

Seong K. Mun: Conceived and designed the experiments; Contributed materials, analysis tools and data; Wrote the paper.

Yue Wang: Conceived and designed the experiments; Contributed materials, analysis tools and data; Wrote the paper.

Data availability statement

Data included in article/supp. material/referenced in article.

Formatting of funding resources

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

Authors are grateful for technical assistance provided by Mr. Peter Li while he was with Open Source Electronic Health Record Alliance, Arlington, VA.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.heliyon.2023.e18061.

References

[1] AHIMA, Defining the personal health record, Journal of AHIMA 76 (6) (2005) 24–25.
[2] Y. Dong, S.K. Mun, Y. Wang, Blockchain-enabled next generation access control, in: J.P.A. Prieto, P. Leitão, A. Pinto (Eds.), BLOCKCHAIN 2021; 2021 September 03. Lecture Notes in Networks and Systems, Springer, Cham, 2022.
[3] Personal health records and the HIPAA privacy rule [Internet] [cited 2022 Apr 23]. Available from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.
[4] Key Considerations, Venesco and Personal Health Records Community of Practice, Venesco LLC, (ONC) OotNCfHI, 2015. Report No.: Contract # 14-233-SOL-00533.
[5] A. Bhattacharjya, The difference between EHR and PHR [Internet] [cited 2022 Oct 8]. Available from: https://www.medicalrecords.com/2021/10/01/blog/the-difference-between-ehr-and-phr.
[6] What is an electronic health record (EHR)? [Internet] [cited 2022 Oct 8]. Available from: https://www.healthit.gov/faq/what-electronic-health-record-ehr.
[7] ONC, Patient-generated health data [cited 2022 Oct 18]. Available from: https://www.healthit.gov/topic/scientific-initiatives/patient-generated-health-data.
[8] Rogerson Fairweather, A moral approach to electronic patient records, Med. Inf. Internet Med. 26 (3) (2001) 219–234.
[9] CFR 160.103 Definitions, 45 CFR 160.103.
[10] Covered entities and business associates [Internet]: U.S. Department of Health & Human Services; [cited 2021 May 18]. Available from: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.
[11] D. McGraw, J.X. Dempsey, L. Harris, J. Goldman, Privacy as an enabler, not an impediment: building trust into health information exchange, Health affairs (Project Hope) 28 (2) (2009) 416–427.
[12] K. Beasley, D. Fischer-Sanchez, Do your patients know how their data is being used? [Internet] 2021 [cited 2022 Apr 23]. Available from: https://www.willistowerswatson.com/en-US/Insights/2021/05/patient-consent-management-for-healthcare-data-reuse.
[13] M.P. Tully, K. Bozentko, S. Clement, A. Hunn, L. Hassan, R. Norris, et al., Investigating the extent to which patients should control access to patient records for research: a deliberative process using citizens' juries, J. Med. Internet Res. 20 (3) (2018) e112.
[14] L. Cardillo, F. Cahill, H. Wylie, A. Williams, J. Zylstra, A. Davies, et al., Patients' perspectives on opt-out consent for observational research: systematic review and focus group, Br. J. Nurs. 27 (22) (2018) 1321–1329.
[15] T. Pietrzykowski, K. Smilowska, The reality of informed consent: empirical studies on patient comprehension—systematic review, Trials 22 (1) (2021) 57.
[16] O. O'Neill, Some limits of informed consent, J. Med. Ethics 29 (1) (2003) 4–7.
[17] D. Shaw, Care.data, consent, and confidentiality, Lancet (London, England) 383 (9924) (2014) 1205.
[18] K. Spencer, C. Sanders, E.A. Whitley, D. Lund, J. Kaye, W.G. Dixon, Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study, J. Med. Internet Res. 18 (4) (2016) e66.
[19] F. Albalwy, A. Brass, A. Davies, A blockchain-based dynamic consent architecture to support clinical genomic data sharing (ConsentChain): proof-of-concept study, JMIR Med Inform 9 (11) (2021), e27816.
[20] C. Thapa, S. Camtepe, Precision health data: requirements, challenges and existing techniques for data security and privacy, Comput. Biol. Med. (2021) 129.
[21] K.K. Kim, P. Sankar, M.D. Wilson, S.C. Haynes, Factors affecting willingness to share electronic health data among California consumers, BMC Medical Ethics [Internet] 18 (1) (2017) 1–10.
[22] M.A. Stone, S.A. Redsell, J.T. Ling, A.D. Hay, Sharing patient data: competing demands of privacy, trust and research in primary care, Br. J. Gen. Pract. : J. Roy. Coll. Gen. Pract. 55 (519) (2005) 783–789.
[23] L.J. Damschroder, J.L. Pritts, M.A. Neblo, R.J. Kalarickal, J.W. Creswell, R.A. Hayward, Patients, privacy and trust: patients' willingness to allow researchers to access their medical records, Soc. Sci. Med. 64 (1) (2007) 223–235.
[24] Y. Dong, S.K. Mun, Y. Wang, Perspective chapter: blockchain-enabled trusted longitudinal personal health record, in: M. Vardan (Ed.), Blockchain, IntechOpen, Rijeka, 2022. Ch. 3.
[25] W.T. Jahn, The 4 basic ethical principles that apply to forensic activities are respect for autonomy, beneficence, nonmaleficence, and justice, J Chiropr Med 10 (3) (2011) 225–226.
[26] J. Garbis, J.W. Chapman, Zero Trust Security : an Enterprise Guide, Apress, Berkeley, CA, 2021, https://doi.org/10.1007/978-1-4842-6702-8 [cited 2022 4/23]. Available from:.
[27] A. Sahai, B. Waters, Fuzzy Identity-Based Encryption. Advances in Cryptology – EUROCRYPT 2005, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 457–473.
[28] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data. Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
[29] M. Li, S. Yu, K. Ren, W. Lou (Eds.), Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
[30] Y. Zheng, Privacy-preserving Personal Health Record System Using Attribute-Based Encryption, Worcester Polytechnic Institute, 2011.
[31] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distr. Syst. 24 (1) (2013) 131–143.
[32] M.K. Debnath, S. Samet, K. Vidyasankar, A Secure Revocable Personal Health Record System with Policy-Based Fine-Grained Access Control, Thirteenth Annual Conference on Privacy, Security and Trust, 2015.
[33] M.H. Au, T.H. Yuen, J.K. Liu, W. Susilo, X. Huang, Y. Xiang, et al., A general framework for secure sharing of personal health records in cloud system, J. Comput. Syst. Sci. 90 (2017) 46–62.
[34] M. Sookhak, F.R. Yu, M.K. Khan, Y. Xiang, R. Buyya, Attribute-based data access control in mobile cloud computing: taxonomy and open issues, Future Generat. Comput. Syst. 72 (2017) 273–287.
[35] V.C. Hu, D.F. Ferraiolo, D.R. Kuhn, Assessment of Access Control Systems, NIST, Gaithersburg, MD 20899-8930, 2006.
[36] P. Samarati, S.C. di Vimercati, International School on Foundations of Security AD. Access control: policies, models, and mechanisms, Lect. Notes Comput. Sci. 2171 LNCS (2001) 137–196.
[37] C.E. Landwehr, Formal models for computer security, ACM Comput. Surv. 13 (3) (1981) 247–278.
[38] P. Jaehong, S. Ravi, Proceedings of the Seventh ACMsAcm, Technologies. Towards Usage Control Models: beyond Traditional Access Control. ACM, 2 Penn Plaza, 0701, Suite 701, New York, NY 10121, 2002.
[39] IBM. Hyperledger fabric a blockchain platform for the enterprise [Internet] [cited 2022 May 23]. Available from: https://hyperledger-fabric.readthedocs.io/en/latest/.
[40] D.F. Ferraiolo, S.I. Gavrila, W. Jansen, P.E. Stutzman, Policy Machine: Features, Architecture, and Specification, NIST, 2015.
[41] X. Ietf. Internet, 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 2003.
[42] HL7, Fast Healthcare Interoperability Resources, HL7, 2019.
[43] Veterans health information systems and technology architecture (VistA) [cited 2023 Jan 1]. Available from: https://worldvista.org/.
[44] Synthea(TM) patient generator [Internet] [cited 2022 Apr 21]. Available from: https://github.com/synthetichealth/synthea.
[45] INCITS. Information, Technology - Next Generation Access Control - Functional Architecture (NGAC-FA). ANSI/INCITS 499-2018, American National Standards Institute, 2018.
[46] 44 USC 3552: Definitions, 2020.
[47] HIPAA Privacy Rule [Inernet], U.S. Department of Health & Human Services, 2013 [cited 2022 May 23]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[48] HIPAA Security Rule, U.S. Department of Health & Human Services [cited 2022 May 23]. Available from:, 2013 https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
[49] C.F.R. § 164 Subpart E—Privacy of Individually Identifiable Health Information.
[50] National Academies PressJ. Sharyl, L.A.L. Nass, Lawrence O. Gostin (Eds.), Committee on Health Research and the Privacy of Health Information: the HIPAA Privacy Rule, Institute of Medicine, 2009. Beyond the hipaa privacy rule: enhancing privacy, improving health through research, http://www.nap.edu/catalog/12458.html.
[51] CMS interoperability and patient access final rule, 42 CFR Parts 406, 407, 422, 423, 431, 438, 457, 482, and 485, 2020.
[52] ONC Cures Act Final Rule, 45 CFR Parts 170 and 171 RIN 0955-AA01, 2020.
[53] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, et al., Hyperledger Fabric: a Distributed Operating System for Permissioned Blockchains. Proceedings of the Thirteenth EuroSys Conference; Porto, Association for Computing Machinery, Portugal, 2018. Article 30.
[54] The Go project [Internet] [cited 2022 Apr 23]. Available from: https://go.dev/.
[55] S. Posnack, Health interoperability outcomes 2030 [Internet] 2021 [cited 2022 Apr 23]. Available from: https://www.healthit.gov/buzz-blog/interoperability/health-interoperability-outcomes-2030.
[56] M. Gur-Arie, The history of healthcare interoperability [Internet] 2013 [cited 2022 January 2nd]. Available from: https://hitconsultant.net/2013/04/11/history-of-healthcare-interoperability/.
[57] F. Rezaeibagha, W. Khin Than, W. Susilo, A systematic literature review on security and privacy of electronic health record systems: technical perspectives, Health Inf. Manag. J. 44 (3) (2015) 23–38.
[58] N.A. Azeez, C.V. der Vyver, Security and privacy issues in e-health cloud-based system: a comprehensive content analysis, Egyptian Informatics Journal 20 (2) (2019) 97–108.
[59] B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020).
[60] H. Guo, W. Li, M. Nejad, C.-C. Shen, A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-Based Cryptographic Mechanisms, 99, IEEE Transactions on Network and Service Management, 2022.
[61] GDPR information [Internet] [cited Apr 19 2023]. Available from: https://gdpr-info.eu/recitals/no-35/.
[62] Neo4j graph database [Internet] [cited 2022 Apr 23]. Available from: https://neo4j.com/product/neo4j-graph-database/.