IntechOpen

Book Chapter

Perspective Chapter: Blockchain-enabled Trusted Longitudinal Personal Health Record

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

Corresponding Author:
Yue Wang, PhD
Virginia Polytechnic Institute and State University
Email: yuewang@vt.edu

Abstract

In the United States, longitudinal personal health record (LPHR) adoption rate has been low in the past two decades. Patients' privacy and security concern is a major roadblock. Patients like to control the privacy and security of their own LPHR distributed across multiple information systems at various facilities. However, little is known how a scalable and interoperable LPHR can be constructed with patient-controlled security and privacy that both patients and providers trust. As an effort to increase LPHR adoption rate and improve the efficiency and quality of care, we propose a blockchain-enabled trusted LPHR (BET-LPHR) design in which security and privacy are protected while patients have full control of the access permissions. Two limitations associated with the proposed design are discussed. Options and practical resolutions are presented to stimulate future research.

Keywords: longitudinal personal health record, security, privacy, confidentiality, permissioned blockchain.

1. Introduction

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, 3). Building electronic health record (EHR) was required by "the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" (4). The first "HIPAA Privacy Rule was released" (4) to "improve privacy standards and to restrict the disclosure of Protected Health Information (PHI) and personal identifiers to unauthorized individuals"(4). In 2009, "the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) was enacted" (5) to remediate a loophole in HIPAA Privacy Rule and promote personal health record (PHR). Untethered (cross-organizational) (6) PHR has been a preferred choice of building LPHR (6). LPHR is attractive to patients because patients can have holistic view of their health information that are scattered in multiple information systems at various facilities. Federal agencies and local governments have been promoting PHR adoption in the past two decades with numerous “laws and regulations, incentives, and penalties” (3, 7, 8). However, “the LPHR adoption rate has been low” (3, 8) in the United States. A.A. Abd-alrazaq et al found out that “patients’ privacy and security concerns is a major negative factor impacting LPHR adoption” (3, 7). Patients like to fully control privacy and security of their own LPHR (3, 7). “However, little is known how to model and construct a scalable and interoperable LPHR with patient-controlled security and privacy that both patients and providers trust” (3). Solving this problem is “considered important to increase LPHR adoption rate and improve the efficiency as well as the quality of care” (3).

To protect the security and privacy of LPHR, encryption is an intuitive and good choice of solution (9-16). Encryption can prevent external security attack, however, it cannot defend against insider threat (3, 17). We argued that insider threat can be remediated via a secure access control model that is implemented correctly at user or session or process level (3, 18, 19). Combining access control model with encryption is a better resolution. Traditional access control model, in which users are well known, has been used to couple with attribute-based encryption (ABE) as an approach. However, in PHR systems, users can be known or unknown. To overcome this problem, we proposed next generation access control which offers “open access surroundings” where “users can be centrally known or unknown”(3). We chose the “National Institute of Standards and Technology (NIST)” “Next Generation Access Control (NGAC)” (20), a type of “attribute-based access control (ABAC)” model (3, 21). Nevertheless, NGAC suffers a race condition in distributed system. This led to our proposal of a “novel Blockchain-enabled Next Generation Access Control (BeNGAC) model” (3) using permissioned blockchain that can ease the race condition. We explained the merits of the new model with additional benefits brought by blockchain technology. We offered the freedom of choice of encryption methods to PHR generators. With BeNGAC as the core of the LPHR access control mechanism, we designed the BET-LPHR that both patients and providers can trust. We discussed two application limitations of the design: a) when the secret private key is lost; b) when the patient cannot directly authorize the access. Possible solutions are offered to solve the limitations. We also compared our approach with prior works.

2. LPHR Requirements

The LPHR requirements are summarized in Table 1.

Requirements	Interpretation
Security: Availability	LPHR “is accessible and usable on demand by authorized persons”(22)
Security: Integrity	LPHR “is not altered or destroyed in an unauthorized manner”(22)
Security and Privacy: Confidentiality	Disallow unauthorized use and disclose of LPHR
Privacy	Use or disclose of LPHR either requires authorization from patients or is obligated to local, state, or federal laws (23, 24)

Authorization	Patients have full control of authorizing LPHR access to other health care providers.
Tamper resistance	Automatically detect and prevent any unauthorized modification.
Access Auditability	Access to LPHR is auditable.
Scalability	LPHR system is enterprise scalable.
Distributedness	LPHR is distributed in EHR vendors and patient's PHR.
Interoperability	LPHR allows share information with other EHRs and stakeholders.
Integration	LPHR allows integrate with smart and wearable personal devices.

Table 1. LPHR Requirements

3. BeNGAC

Encryption is a good choice of protecting privacy and confidentiality of PHR on premises and in the cloud. Invented by Amit Sahai and Brent Waters(9), ABE and its extensions have been researched extensively and applied to PHR confidentiality and privacy protection (9-16). However, encryption alone cannot prevent insider threat (3, 17). Miller & Tucker (17) suggested applying access control to remediate insider threat (3, 17). Akshay Tembhare et. al. combined role-based access control (RBAC) model with ABE to protect PHR in the cloud (25). However, RBAC is a type of traditional access control method that users are known. PHR users can be centrally known or unknown, in which next generation access control model is a better fit. This led us to choose the NIST's NGAC as an authorization model. Furthermore, NGAC meets the LPHR distributedness requirement because NGAC provides unified access control policies and resources reinforce the policies are distributed (3, 21). Moreover, NGAC is scalable at enterprise level (21) which "fulfills the LPHR scalability requirement" (3).

Nevertheless, in distributed system, NGAC suffers a "race condition" when access control policies are centralized while decisions making processes are localized (26). To solve this problem, we proposed a decentralized yet distributed access control policy expression unit by using permission blockchain technology Hyperledger Fabric (HF) (3). We introduced a novel BeNGAC model (3). In LPHR, patients and providers trust each other, which matches the property of permissioned blockchain. The "race condition" in NGAC is eased by HF "concurrency control" (3, 27) contributed by "HF consensus" (3, 27). The access control policy information is immutable by inheriting HF's immunizability property. The blockchain transaction audit logs are on chain while the access control policies are stored in private off-chain database (3). Furthermore, NGAC access control policies compensate HF's weak confidentiality protection. The BeNGAC architecture is sketched in Figure 1. "Policy enhancement point (PEP), policy decision point (PDP), event processing point (EPP), and resource access point (RAP)" (3, 26) are distributed and act locally. The policy administration unit (PAU) consists of blockchain-enabled policy administration point (BePAP) and blockchain-enabled policy information point (BePIP) that are decentralized. An application requests to access BET-LPHR. The request is processed by PEP. PEP relays the request to decision maker PDP. PDP queries the policy database BePIP via BePAP. The request is processed and a grant or deny decision is sent to the application via PEP. If the decision is to “allow”, the application will send a request to access the BET-LPHR through RAP.

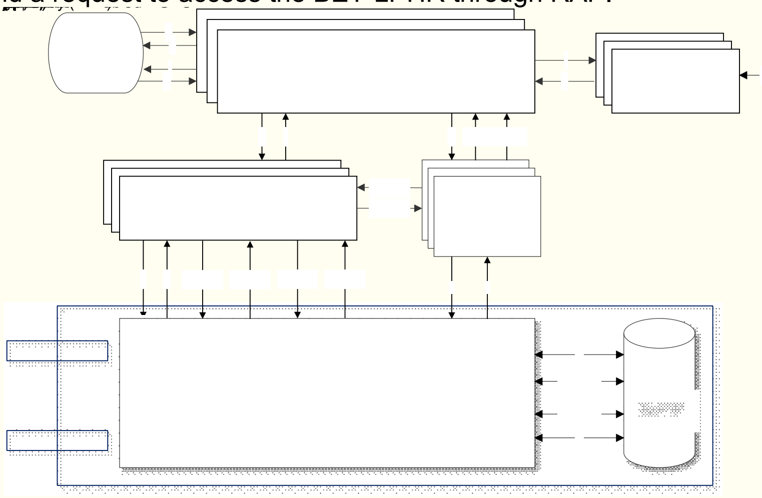

Figure 1. BeNGAC Architecture (3, 26)

4. BET-LPHR

The BET-LPHR consists of two partitions of data: 1) patient self-generated PHR such as data from personal wearable devices; 2) PHR data replicated from the EHRs the patient has visited.

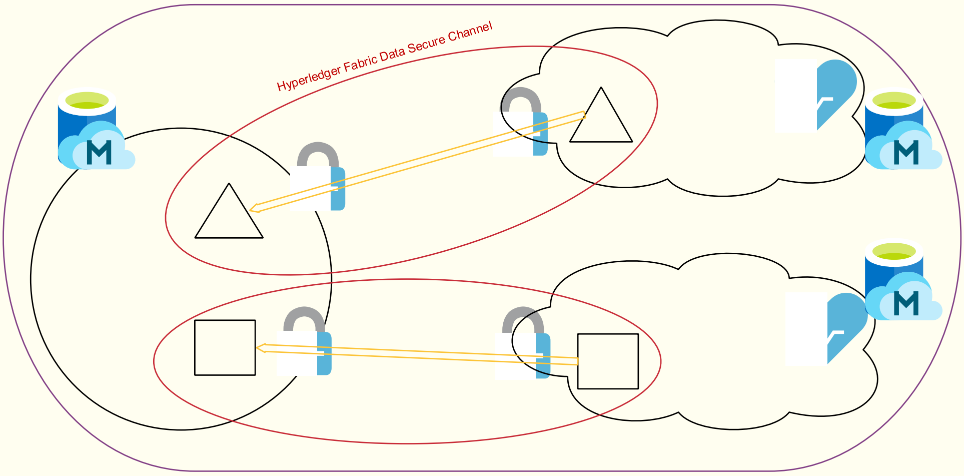

Figure 2. BET-LPHR Model

Figure 2 illustrates the BET-LPHR model. VistA_EHR_A and VistA_EHR_B represent the EHR providers that the patient has been visited. The patient, VistA_EHR_A, and VistA_EHR_B form a trusted network and connected by HF BeNGAC policy secure channel. The patient (considered as one organization in this setting) and the two EHR organizations share the same access control policies. “The patient has full control of granular permissions on his or her own LPHR” (3) using the shared access control policies that are realized via a Web-based interface presented to the patients. “The blockchain based peer-to-peer

BeNGAC database avoids racing condition during policy reinforcement"(3). The data sharing operates on a different type of HF communication channel, HF data secure channel. The patient and VistA_EHR_A constitute a trusted HF data secure channel. The patient's PHR data in VistA_EHR_A (triangle shape) is copied (disclosed) to the patient's BET-LPHR. Similarly, BET-LPHR has a PHR copy (square shape) from VistA_EHR_B on a different HF data secure channel. BET-LPHR is distributed to three organizations. Among the trusted HF data sharing channel, BET-LPHR is decentralized (or peer-to-peer).

At a high level, BET-LPHR data flow is summarized in Figure 3. The patient and the EHR organizations are communicated via Fast Healthcare Interoperability Resources (FHIR) interface to ensure interoperability. "Digital certificate guarded secure authentication and BeNGAC policies meet the LPHR security and privacy requirements" (3). Both NGAC and HF are enterprise scalable, so BET-LPHR is enterprise scalable to meet LPHR scalability requirement. The authentication to BET-LPHR relies on asymmetric cryptography private keys. Data in transit is encrypted by the public key and protected by transport layer security (TLS). Data at rest in EHR's silos are protected by the encryption methods the EHR organizations freely choose.

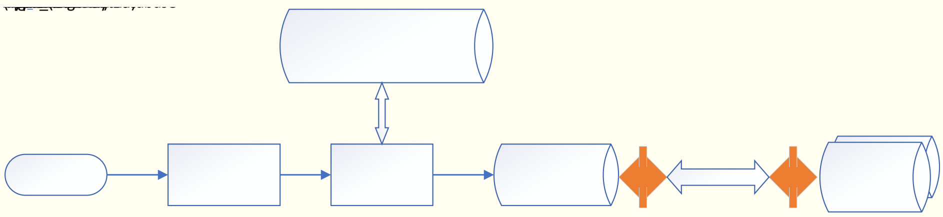

Figure 3. BET-LPHR Architecture

BET-LPHR offers unique event processing capabilities, such as prohibition or obligation, that is inherited from BeNGAC. This fills a gap in traditional access control model when handling insider threat. For example, in RBAC, a doctor is authorized to read a patient's record, but a nurse is not. The RBAC does not prohibit the doctor copy and paste a record to a file that the nurse has permission to read. In BET-LPHR, this is remediated by the prohibition policy as the following (3):

"Configuration Rule 1:
When process performs where do create
Configuration Rule 2:
When process performs do create "

The doctor authenticates with a user session and the session launched a read (*r*) process (*p*). When the process *p* performs a *read* or *copy* operation on an object which is assigned to the patient's medical record (med_red) attribute, it triggers a prohibition condition to deny writing to an object that is not the object being read.

The LPHR requirements are fulfilled by the BET-LPHR designed and are summarized in *Table 2*.

Requirements	**NGAC**	**HF Blockchain**	**FHIR**
Security	X	X	

Privacy, Confidentiality	X	Some	
Integrity: changes to a LPHR - Tamper Resistance	X	X	
Access Audit		X	
Scalability	X	X	
Distributedness	X	X	
Interoperability and Integration			X

Table 2. BET-LPHR Requirements Fulfillment

5. Limitations and alternatives

There are few limitations of the BET-LPHR design. Some are inherited from EHR and PHR, others are from blockchain technology itself.

5.1 When BET-LPHR Owner Lost the Secret Private Key

From authentication to authorization, owner's secret private key is essential to unlock the patient's BET-LPHR as a passport to securely administrate BET-LPHR. Being a problem inherited from the blockchain technology itself, losing the secret private key presents a barrier.

We propose a separate blockchain-enabled SecureKey recovery process with a secure login portal using the "BeNGAC and RBAC Separation of Duty (SoD) capability" (3). Accessing to this portal requires strong multi-factor authentication (MFA) with Fast Identity Online (FIDO) 2.0 biometrics (28). The patient secret key pair is generated by the key administrator and delivered to the owner in a secure manner. At the same time, a recovery key pair is also generated and sent to the owner. The key administrator and the owner possess the recovery public key, but only the owner has the BET-LPHR patient secret key pair and recovery private key. The keys roles and permissions are described in Table 3.

Role	Key Administrator	BET-LPHR Patient/Owner
BET-LPHR Patient Secret Key Pair		Secure Public Key ()
		Secure Private Key ()
Recovery Key Pair	Recovery Public Key ()	Recovery Public Key ()
		Recovery Private Key ()

Table 3. Roles of Key Administrator and BET-LPHR Patient/Owner

At the BET-LPHR patient key pair generation time, a copy of the secret private key) is encrypted with the recovery public key (). The encrypted secure private key) and recovery private key (are stored in a *Blockchain-Enabled SecureKey* database with read only permission.

When the BET-LPHR owner lost the secure private key , there are two scenarios for the BET-LPHR owner to recover the key (Figure 4):

- **Scenario #1**. If the BET-LPHR owner has the recovery private key , the BET-LPHR owner can send a key recovery request through a private key recovery login Web page. The patient will be authenticated with the recovery private key . Once authenticated, the patient will go through a multi-factor authentication process to answer some secure questions to prove the identity and then retrieve the encrypted secure private key . The secure private key can be recovered by using .

- **Scenario #2**. If the BET-LPHR owner lost both secure private key and recovery private key , the owner can request the Key Administrator to recover the encrypted private key. The owner must go through an identity proof process. Once the owner is identified as the owner of the secure private key and recovery private key , the policy administrator will create a one-time login credential for the owner to login to the private key recovery login Web page, and assign the owner to a user attribute which has read access to the encrypted secure private key and the recovery private key . For example, Joyce Taylor is assigned to Joyce_Taylor_Admin_Patient_Recovery attribute, which has capability of reading the Joyce_Taylor_Encypted_Secure_Private_Key and Joyce_Taylor_Recovery_Private_Key. The following BeNGAC obligation rules apply:
    - **When** Key_Admin write to Joyce_Taylor_Encrypted_Secure_Private_Key **do**
        - Create u_deny (Key_Admin) read from Joyce_Taylor_Encrypted_Secure_Private_Key
        - Create u_deny (Key_Admin) assign to Joyce_Taylor_Admin_Patient_Key_Recovery
        - Create u_deny (Key_Admin) assign to Joyce_Taylor_Key_Selft_Recovery
    - **When** Key_Admin write to Joyce_Taylor_Recovery_Private_Key **do**
        - Create u_deny (Key_Admin) read from Joyce_Taylor_Recovery_Private_Key
        - Create u_deny (Key_Admin) assign to Joyce_Taylor_Admin_Patient_Key_Recovery
        - Create u_deny (Key_Admin) assign to Joyce_Taylor_Key_Selft_Recovery
    - **When** Joyce_Taylor proves identity, **do** assign Joyce to Joyce_Taylor_Admin_Patient_Recovery

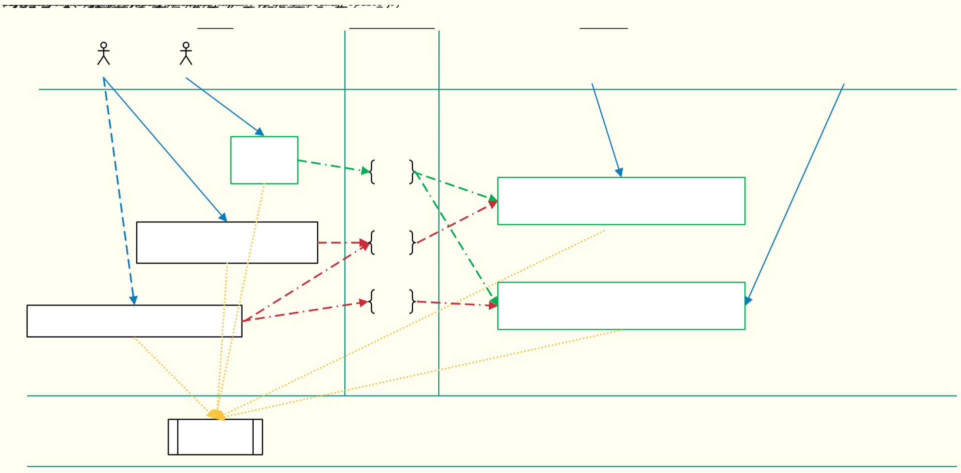

Figure 4. Secure Private Key Recovery

5.2 When the BET-LPHR Owner Cannot Directly Authorize the Access to the Third Party

"In general, the BET-LPHR owner can grant permission to a legitimate third party, for instance a specialty doctor he or she will visit during a referral encounter. There are situations such as emergency departments visit, where BET-LPHR access is desired by the ER physicians to make better decision of a care plan by using the patient's BET-LPHR information such as medications taken, allergy conditions, recent doctors' visits, chronic diseases, and recent laboratory test results (29). However, as a limitation that the patient need to directly grant the permission of BET-LPHR to the doctors in ER, it is not uncommon that the patient is unconscious and cannot authorize the access of his or her BET-LPHR to the doctors in ER facility" (3).

We propose a viable solution using BeNGAC RBAC and Discretionary Access Control (DAC) policies with obligations in the following example (Figure 5):

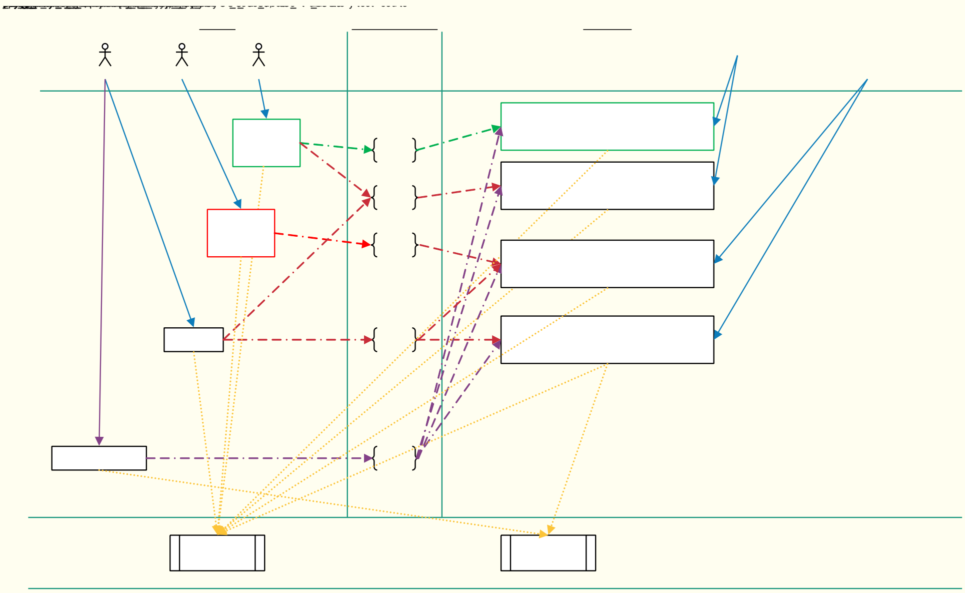

Figure 5. Indirectly Authorize BET-LPHR Access to ER Physicians

In this scenario, an object attribute Joyce_Taylor_SharedWith_ER_Doctor is created during user profile initialization. A user attribute ER_Doctor is also configured with read only permission on Joyce_Taylor_SharedWith_ER_Doctor. The patient's subset of BET-LPHR that are required during an emergency department visit are assigned to the object attribute Joyce_Taylor_SharedWith_ER_Doctor. The information includes the current medications taken, patient's chronic allergy conditions, doctors' visits in the past 3 months, patient's chronic diseases information, and laboratory test results in the past 90 days. The information is automatically assigned to the Joyce_Taylor_SharedWith_ER_Doctor when a new BET-LPHR record is added either by the encounter during doctor's visit in VistA_EHR_A or when patient records a new self-generated health record to the BET-LPHR. Additionally, a retrospective process can run on demand to assign or unassign patient's BET-LPHR to the Joyce_Taylor_SharedWith_ER_Doctor.

When the patient is in an emergency department and lost consciousness, the ER physician can send a request to the patient's BET-LPHR administrator along with doctor's identification for a temporary account in patient's BET-LPHR. The doctor (Edward) with this account is assigned to the ER_Doctor role. The account will be disabled after 72 hours of account creation. The following obligation rules are reinforced:

- **When** Jocye_Taylor's new medical record is in ["allergy conditions, recent doctors' visits, chronic diseases, recent laboratory test results"] (3) **do** assign new_medical_record to Joyce_Taylor_SharedWith_ER_doctor.
- **When** new medication is prescribed to Joyce_Taylor **do** assign the new_medication_info to Joyce_Taylor_SharedWith_ER_doctor
- **When** a doctor is assigned to ER_Doctor attribute **do** create u_disable the account after 72 hours.

5.3 Comparison with Prior Work

5.3.1 HealthChain

Hylock & Zeng presented HealthChain (30), a proof-of-concept study of patient-centric health record management framework based on blockchain technology. The authors argued patients' health information in current tethered EHRs are inclined to fragmentation due to distributedness of patient records, which leads to poor care coordination. Hylock & Zeng pointed out ONC information blocking discouraged patients' engagement. Therefore, the authors proposed a mixed-block permissioned blockchain solution coupled with FHIR, the interoperability standard. The mixed-block blockchain consists of immutable logs blocks and editable patient blocks, while large size multimedia data are kept off chain at EHR's silos and only reference pointers are stored in patient blocks. HealthChain acts as "an interface between patients and providers or payers" (30). The authors claimed security was ensured by implementing permissioned blockchain, and only trusted parties including patients could make changes. The privacy or confidentiality was protected by smart contract and 2-party proxy re-encryption decryption.

In HealthChain, the patient data are on the blockchain, which motivated the authors to redesign the data allocation strategy with patient block data consolidation for a certain patient via Chameleon hashing (31). The blockchain patient block is redactable (or editable). On one hand, Hylock & Zeng regarded consensus and immutability, which are the core properties of blockchain technology, as shortcomings of computing performance and cost barrier when data blocks are being modified (30). The authors argued modifications to existing patient blocks could avoid costly consensus. On the other hand, the authors stated using blockchain and smart contacts in HealthChain could meet the HIPAA privacy and security rules requirements. Therefore, if core features of blockchain technology, consensus and immutability, were identified as roadblocks to HealthChain sketch, the applicability of blockchain technology to such a design should be reconsidered. Furthermore, keeping patients' data on-chain is not practical at enterprise level. This design could not scale when number of patients and providers are increasing.

Compared with HealthChain, BET-LPHR patient data is off-chain in a "private database while the audit logs are on-chain"(3). BET-LPHR is enterprise scalable. BET-LPHR provides privacy and confidentiality protection via BeNGAC.

5.3.2 MedRec

In August 2016, Ekblaw, Azaria, Halamka, & Lippman prototyped an Ethereum blockchain based MedRec 1.0 (32, 33) for EHR and medical research data to engage patients as agencies to their own health records. MedRec acts as an interface between providers' EHRs and patients. The patients EHRs data are siloed at providers' data centers, while patients are presented a local cached database to patients' records. Through MedRec patient-provider relationship (PPR) smart contract, a certain degree of fine granular access control to patients' health records is achieved by checking on or off fields of medical records steered by patients via a graphical application portal. The MedRec Summary Smart Contract (SSC) weaves PPR smart contracts together to form a holistic view of a patient's medical records from all providers by integrating the reference points to PPRs. The SSC is persistent on the blockchain, which offers flexibility to patients or providers to re-join the network and recover from a system disaster. The MedRec Registrar Smart Contract (RSC) links a patient's existing EHR participant ID to an Ethereum cryptographic public key identifier. The identification registration process is controlled by limited authorization institutions. In MedRec, any changes to a patient's records on a provider's EHR requires an acknowledgment of acceptance or rejection from patient's client. In MedRec, the authors argued the authentication, confidentiality, and data sharing accountability are managed by blockchain smart contracts.

There are few drawbacks in MedRec design. Firstly, when creating a new medical record in provider's EHR, MedRec requires the provider to compose a query string that retrieves that part of data and associate a hash of the query output to guarantee data integrity. However, before a patient accepts this new change, this new record is not in patient's holistic view nor treated as patient's genuine data by the patient. At this point, a hacker (either internal or external) can disclose this new record to a third party without notifying the patient, which violates privacy and confidentiality of the patient record. Secondly, since any change to a patient's records on provider's side requires patient's communication to accept or deny the change, if for some reason, the patient cannot respond to the communication, the authors did not explain the results of those affected records. Thirdly, Proof-of-Work (PoW) was implemented as a mining approach, which consumes excessive computing energy.

In 2019, Nchinda, Cameron, Retzepi, & Lippman introduced a new architectural design of MedRec 2.0 (34). The MedRec 2.0 replaced PoW with computing cost saving Proof-of-Authority (PoA) based on the trusted participants of EHR data providers on the blockchain network. The MedRec 2.0 is an open-source solution, claimed by authors to be a robust approach with small system resource consumption overhead to the existing EHRs. However, the scalability needs to be tested when more health care community users adopt the solution.

In contrast to MedRec, BET-LPHR does not require the patient to confirm denying or accepting changes when adding a health record. Furthermore, BET-LPHR uses HF consensus so it eliminated the consensus overhead of PoW or PoA.

6. Conclusions

In this chapter, we presented a scalable and interoperable BET-LPHR solution to solve a longstanding PHR problem. Patients get benefits of controlling the security and privacy of their own LPHR when sharing the information with trusted health care providers. The permission control autonomy is achieved via

BeNGAC. The BET-LPHR is built on top of BeNGAC network with a FHIR interface so it is interoperable with other EHRs. Both BeNGAC and BET-LPHR are enterprise scalable. The BET-LPHR is distributed yet decentralized and tamper resistant with auditable changes. We discussed two limitations of the solution when owner lost the private key or cannot directly authorize the access to BET-LPHR. Also, the current HF version supports up to 100 organizations (27) on the same policy or data secure channel, which can present a limit when a patient wants to include more than 99 EHR organizations to BET-LPHR on the same secure policy channel. We leave this for future research.

Acknowledgments

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

References

1. AHIMA. Defining the personal health record. Journal of AHIMA. 2005;76(6):24-5.

2. 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.

3. Dong Y, Mun SK, Wang Y. Blockchain-enabled next generation access control. In: Prieto J. PA, Leitão P., Pinto A., editor. BLOCKCHAIN 2021; 2021 September 03. Lecture Notes in Networks and Systems: Springer, Cham; 2022.

4. HIPAA history [Internet] [cited 2022 May 23]. Available from: https://www.hipaajournal.com/hipaa-history/.

5. *H.R.1 - American Recovery and Reinvestment Act of 2009*, PLAW-111publ5 (2009).

6. Key considerations, venesco and personal health records community of practice. Venesco LLC, (ONC) OotNCfHI; 2015. Report No.: Contract # 14-233-SOL-00533.

7. Abd-Alrazaq AA, Bewick BM, Farragher T, Gardner P. Factors that affect the use of electronic personal health records among patients: A systematic review. Int J Med Inform. 2019;126:164-75.

8. ONC. Office-based physician electronic health record adoption [Internet] 2017 [cited 2022 May 23]. Available from: https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php.

9. Sahai A, Waters B. Fuzzy identity-based encryption. Advances in Cryptology – EUROCRYPT 2005: Springer Berlin Heidelberg : Berlin, Heidelberg; 2005. p. 457-73.

10. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security; 2006. p. 89-98.

11. Li M, Yu S, Ren K, Lou W, editors. Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings; 2010; Berlin, Heidelberg: Springer Berlin Heidelberg.

12. Zheng Y. Privacy-preserving personal health record system using attribute-based encryption: Worcester Polytechnic Institute; 2011.

13. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems. 2013;24(1):131-43.

14. Debnath MK, Samet S, Vidyasankar K. A secure revocable personal health record system with policy-based fine-grained access control. Thirteenth Annual Conference on Privacy, Security and Trust 2015.

15. Au MH, Yuen TH, Liu JK, Susilo W, Huang X, Xiang Y, et al. A general framework for secure sharing of personal health records in cloud system. Journal of Computer and System Sciences. 2017;90:46-62.

16. Sookhak M, Yu FR, Khan MK, Xiang Y, Buyya R. Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. Future Generation Computer Systems. 2017;72:273-87.

17. Miller AR, Tucker CE. Encryption and the loss of patient data. Journal of Policy Analysis and Management. 2011;30(3):534-56.

18. Samarati P, di Vimercati SC, International School on Foundations of Security A, Design. 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:137-96.

19. Landwehr CE. Formal models for computer security. ACM Computing Surveys (CSUR). 1981;13(3):247-78.

20. INCITS. *Information technology - Next Generation Access Control - Functional Architecture (NGAC-FA)*. ANSI/INCITS 499-2018: American National Standards Institute; 2018.

21. Hu VC, Ferraiolo DF, Kuhn DR. Assessment of access control systems. Gaithersburg, MD 20899-8930: NIST; 2006.

22. HIPAA security rule [Internet]: U.S. Department of Health & Human Services; 2013 [cited 2022 May 23]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

23. *CMS interoperability and patient access final rule*, 42 CFR Parts 406, 407, 422, 423, 431, 438, 457, 482, and 485 (March 9, 2020).

24. *ONC Cures Act Final Rule*, 45 CFR Parts 170 and 171 RIN 0955-AA01 (March 9, 2020).

25. Tembhare A, Sibi Chakkaravarthy S, Sangeetha D, Vaidehi V, Venkata Rathnam M. Role-based policy to maintain privacy of patient health records in cloud. The Journal of Supercomputing : An International Journal of High-Performance Computer Design, Analysis, and Use. 2019;75(9):5866-81.

26. Ferraiolo DF, Gavrila SI, Jansen W, Stutzman PE. Policy machine: features, architecture, and specification. NIST; 2015.

27. IBM. Hyperledger fabric a blockchain platform for the enterprise [Internet] [cited 2022 May 23]. Available from: https://hyperledger-fabric.readthedocs.io/en/latest/.

28. FIDO alliance [Internet] [cited 2022 May 21]. Available from: https://fidoalliance.org/.

29. Wilcox AB, Shen S, Dorr DA, Hripcsak G, Heermann L, Narus SP. Improving access to longitudinal patient health information within an emergency department. Applied clinical informatics. 2012;3(3):290-300.

30. Hylock RH, Zeng X. A blockchain framework for patient-centered health records and exchange (healthchain): evaluation and proof-of-concept study. J Med Internet Res. 2019;21(8):e13592.

31. Ashritha K, M S, Kv L, th International Conference on Advanced C, Communication Systems Coimbatore IMM. Redactable blockchain using enhanced chameleon hash function. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS): IEEE; 2019. p. 323-8.

32. Ekblaw A, Azaria A, Halamka JD, Lippman A. A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data. In: Lab MM, Center BIDM, editors. 2016.

33. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD)2016. p. 25-30.

34. Nchinda N, Cameron A, Retzepi K, Lippman A. MedRec a network for personal information distribution. 2019 International Conference on Computing, Networking and Communications (ICNC); Honolulu, HI, USA2019. p. 637-41.