Fusing Identity Management, HL7 and Blockchain into a Global Healthcare Record Sharing Architecture

Mohammad A. R. Abdeen[1], Toqeer Ali[2]
Islamic University of Madinah
Madinah, Saudi Arabia

Yasar Khan[3]
University of Kuala Lumpur,
Malaysia

M. C.E. Yagoub[4]
School of Electrical Engineering
and Computer Science
University of Ottawa, Canada

***Abstract*—Healthcare record sharing among various medical roles is a critical and challenging research problem especially in today's everchanging global IT solutions. The emergence of blockchain as a new enabling technology brought radical changes to numerous business applications, including healthcare. Blockchain is a trusted distributed ledger that forms a decentralized infrastructure. There have been several proposals regarding the sharing of critical healthcare records over blockchain infrastructure without requiring prior knowledge/trust of the parties involved (patients, service providers, and insurance companies). Another yet important issue is to securely share medical records across various countries for travelling patients to ensure an integrated and ubiquitous healthcare service. In this paper, we present a globally integrated healthcare record sharing architecture based on blockchain and HL7 client. Healthcare records are stored at the hosting country and are not stored on the blockchain. This architecture avails medical records of travelling patients temporarily and after performing necessary authentication. The actual authorisation process is performed on a federated identity management system, such as, the Shibboleth. Though there are similarities with identity management systems, our system is unique as it involves the patient in the permission process and discloses to them the identities of entities accessed their health records. Our solution also improves performance and guarantees privacy and security through the use of blockchain and identity management system.**

***Keywords*—Healthcare; blockchain; electronic health record; identity management; Health Level Seven (HL7)**

I. Introduction

Healthcare record sharing systems (HRS) achieved significant maturity in the past couple of decades. Many works have been reported in the literature that used various techniques to securely store and retrieve Electronic Health Records (EHR) [1]. At the same time, an important aspect is to address the privacy concerns of the users such as the EHR should be made available to specific personnel within a specific time frame [2]. Storing EHR in a globally integrated database is also an open problem [3]. For example, retrieving a patient record, that is stored in a remote HRS system, from a local clinic currently being visited by a patient because HRS systems usually store health records in various non-standard formats. To anonymously store and retrieve records among two different HRS systems a standardized mechanism is provided with Healthcare Level Seven (HL7) standards [4]. Moreover, to release a health record to a specific medical role in a given clinic requires further authorization. Federated Identity Management (FIDM) provides the required framework to achieve this objective. The FIDM systems provide authentication, authorization, and privacy of identity among various organizations that are accessing a specific resource. FIDMs consist of a Service Provider(SP), an Identity Provider (IdP) to provide access to a secure resource among various organizations, and a user that requests that specific resource. One of the critical issues we address in this research emerges from the fact that an attempt to integrate an FIDM and an HL7 system is that, once authorized to access an EHR, user activities will not be traceable. An example of this is when a patient visits a clinic/hospital that he/she is not registered in. Since the clinic is part of the federation, it is allowed to access a EHR of that patient after authorization by an identity provider (IdP). The SP then provides the EHR of the patient to the user. The physician can then make recommendation and prescription to the patient. In case of medication/prescription errors an investigation might be required and evidence can be gathered. The previous setup does not prevent recorded tampering of the HRS system which might result in an unresolvable dispute among parties involved. Fig. 1 shows a simplified sequence diagram for a non-blockchain healthcare record sharing system

The solution to this problem is to allow changes to healthcare records only upon consensus among all parties involved. Blockchains, which is an emerging technology, facilitates this objective. Blockchain is a trusted decentralized system that can perform a transaction among two unknown participants. Blockchains opened a new frontier to develop business applications and is adopted by many applications including healthcare. The aforementioned problem can be rectified by the Blockchain system as it provides a trusted ledger. The ledger keeps track of all the transactions performed by the Blockchain systems. It contains a smart contract, consensus and trusted ledger database. Each transaction on the smart contract is given to the consensus layer which upon agreement of each node in the Blockchain network stores the transaction. The transactions are secured with a hashing algorithm and chains all the previous records stored in the database. In parallel each transaction is stored on a normal database. However, the difference between a normal database and a Blockchain database is that a record cannot be deleted without the consensus of all nodes in the network. Any attempt to tamper with patient records, the system will immediately detect it.

In this work, the authors present a new architecture that employs the concept of federated identity management available by the FIDM and the security and immutability of the Blockchain. The HL7 provides a secure and trusted EHR sharing system. The proposed solution also provides a federation of healthcare systems globally. That is, if a patient is traveling across countries and if he/she requires healthcare service, they will be able to access their health records from anywhere. The remote service provider will be able to retrieve patient's EHR from his/her local database, while preventing tampering to those records. The HRS of the patient home country is known as Home_Station(HS), the authorization provider is recognized as Identity Provider(IdP) and service provider at the remote clinic is RS in the presented solution. Each transaction is recorded on the Blockchain at the RS. The peer nodes in the Blockchain network belong to various organizations that are part of the federation.

We implemented a proof-of-concept of this architecture on the Shibboleth and Hyperledger composer. The necessary customizations are performed on the Shibboleth IdP and the HS. The HS is further integrated with HL7 to retrieve the EHR from the local HRS.

Paper Organization: In this paper we present a framework for global healthcare record retrieval by fusing FIdM, HL7, and Blockchain technologies for the purpose of achieving secure, standardized and tamper free transactions. A proof-of-concept of this framework is implemented on a Hyperledger composer Blockchain with use case scenarios. Section II gives an overview of the related work to the problem we are addressing. Section III gives a background information related to the topic. Section IV gives the implementation details including the architecture and the BNA.

II. Related Work

There has been various attempts to adopt the blockchain framework in healthcare to facilitate better data sharing among providers and replace the data silos model with a decentralized, more secure one. The following is a review of some of this work.

In [5], the author argued that the move to the blockchain platform in the healthcare sector will not be in the near future due to the fact that healthcare providers tend to keep the status quo, that is the technology they invested large amounts of cash for the past years. The authors argues that a more reasonable way is to gradually move form the current centralized healthcare system to the blockchain based one. This can be performed with one of three options, the easiest of which is that the patient be responsible for uploading the healthcare records to the blockchain each time they access the old system. This could result in an incomplete record if patient forgets to perform this manual step.

Ping Zhang et al. [6], demonstrated a blockchain based application - FHIRChain - for secure clinical data sharing and in light of the requirement defined by the "Office of National Coordinator for Health Information Technology" (ONC). The main objective is to achieve secure and scalable data sharing. The authors combined the objective of information sharing, through a blockchain based architecture, with security of personal sensitive information such as identity information and medical records, via public key encryption based digital identity.

The authors implemented a decentralized application (DApp) based on the FHIRChain for a tumor board for the purpose of supporting collaborative clinical decision making. ONC requirements are achieved on this application using various techniques including storing metadata for medical records on the blockchain rather than storing the data itself for better security and scalability. The authors also used a double encryption public key encryption for authenticating access to patient medical records. Consistent medical data formatting is ensured by enforcing the FHIR standard. In [7] the authors proposed the use blockchain for the purpose of data sharing in pervasive social networks (PSN). Secure data sharing is achieved by implementing a modified version of the IEEE 802.15.6 to establish secure connections among wearable body sensors and other devices in the PSN.

In [8] the authors presented a software application, DASH, based on Etherium platform for blockchain based healthcare to facilitate patient/doctor/provider interaction and grant required and necessary access to the parties involved. Software design patterns have been employed in this paper.

In [9] the authors presented a framework called MedRec that manages patient medical records while enables record sharing with authentication and fast editing. The main motivation is that the current electronic health record (EHR) system suffers form interoperability issues among various providers and does not allow patients to have access (read only) to their own records. There has been needs among care providers to share and transfer patient records for better healthcare. The proposed MedRec system is based on the blockchain model.

T.-T. Kuo et. al. [10] discussed health information prediction related to a patient for decision making purposes, such as, whether a patient should be admitted or not. Instead of transferring sensitive patient information, authors proposed the transfer of partially-trained models for the purpose of data prediction. Their proposed system minimizes both the transaction time and the chances of malicious attacks. In [11], the authors has presented a framework to securely share healthcare record among participants.

In [12] the authors proposed a blockchain based architecture for the purpose of achieving precision medicine and for a better clinical trials. The proposed architecture consists of a "new" blockchain built on top of the traditional blockchain.

III. Background

In this section we give an overview of the components of the presented global healthcare architecture.

A. Blockchain

Blockchain is an emerging technology initially introduced by a group of researchers for timestamping digital document so that they can not be tampered with. The concept was redefined in 2008 by Satochi Nakamoto and applied on the area of digital currency and created the first cryptocurrency project, the Bitcoin [13]. Blockchain is a decentralized, distributed ledger where transactions records are stored on a peer-to-peer network rather than a centralized system. This specific architecture

enabled blockchains to provide secure, immutable services with provenance. A blockchain consists of blocks representing transactions. Those blocks are chained together in the sense that each block carries a "fingerprint" of the previous blocks of the chain. Any attempts to change a block will render the whole chain invalid, unless in the case of the availability of an unusual immense computational power to reprogram the entire blockchain, which is nearly impossible. In blockchains, each node (or participant) approves, maintains, and updates new entries. Thus, validating the entries of the blockchain is not the responsibility of a single, centralized entity, but it is the responsibility of everyone participating in the network. This architecture therefore creates a trusted and secure ledger of members whom a priori trust does not necessarily exist [14].

Blockchains consist of the following main components:

- The node: is the hardware machine running the blockchain software
- The transaction: includes information about a specific transaction of the blockchain such as the originator, recipient and the nature of transaction (amount of money in exchange for example)
- The block: is a data structure and the basic building block of the blockchain that wrapped a transaction information and adds extra information about the previous blocks.
- The Miners: any nodes competing to find the required hash to validate a new transaction.
- Consensus: is a set of rules that are agreed upon between all participants for the purpose of approving new transactions.

Various flavors of Blockchains have emerged since its introduction. Initially public Blockchains served the purpose of providing anonymous service such as online retail of participating member of the network. While this had an advantage of flexibility and transaction security, it does not provide information about the identity of the participant. A new version of the Blockchains was introduced that are restricted to a set of users and are called private or permissioned Blockchains [15], [16]. This version is not public but it is restricted to specific users or user categories. Permissioned blockchains provides the advantages of security, immutability and provenance and at the same time provides user identification. Many notable private blockchain platforms exists such as Quorum and Hyperledger Fabric and [16]. Quorum is based on Ethereum which is itself a public blockchain platform. On the other hand, Hyperledger Fabric is a private blockchain that is specifically built for business transactions instead of only cryptocurrency exchange. Private blockchain enable support for general purpose business transactions, such as, Hyperledger Composer [17]. The system includes an access control mechanism to own various assets. In addition, the owners or participants are to be distinctly identified within the blockchain network. Composer provides Restful web services interface to connect third party applications with the blockchain.

The following sections briefly describe the most important aspects and terminology of blockchains:

1) Consensus PoW, PoS: Consensus is a central technique in the working of blockchains. It is a way to reach to a decision among the participants (which can be in tens of thousands) based on specific set of rules to perform/approve a given transaction. There exist several algorithms in the literature but the most known ones are the Proof-of-Work (PoW) and the Proof-of-Stake (PoS).

2) Smart Contract: A smart contract is a program that manages the transfer of assets or digital currency between parties when certain conditions are met. Smart contracts defies the rules and conditions under which this transfer occurs. They also can enforce those rules. Smart contracts can also perform transactions on a wide range of fields such as legal processes or insurance premiums. Smart contracts idea was solidified with the development of the cryptocurrency bitcoin and used the blockchain as a medium to store the terms of the contract. Smart contracts have been used recently to transfer and track property titles. Upon a transaction completion the buyer receives a digital token that can be used as a proof of ownership.

3) Hyperledger Fabric: The Hyperledger is an open source implementation of the blockchain and tools by linux foundation. The Hyperledger fabric is the permissioned blockchain infrastructure of the blockchain originally introduced by IBM.

4) Hyperledger Composer: The Hyperledger framework has several development tools. The Hyperledger composer is one of those tools that help developers build a blockchain business network and create smart contracts. The composer provide a GUI user interface that is called "Playground" which acts as a good starting point for prototyping proof of concept applications.

- **The Business Network Archive** The Business Network Archive (BNA) is a file that contains other file that includes the definition of the business network in the Hyperledger composer. These files include a set of model files, a set of JavaScript files written by the developer based on business analysis and a set of access control files that contains a set of rules that defines the permissions of participants of the network.
- **Restful Web Services** The Restful is an architectural style that defines a set of constraints to perform web services. A Restful web service is a service that complies with those constraints. The Hyperledger Composer avails a REST API to be consumed by HTTP or REST clients that participate in the network.

B. Federated Identity Management System

Access to sensitive information/resource requires user authentication with usually username/password or through biometric systems. Healthcare systems, however, are designed to access its data locally or within their organizational boundaries. Most healthcare organizations have their own system for patient record keeping which might be shared by multiple individuals (physicians, laboratories, technicians) in multiple places. In places/countries receiving millions of tourists every year, accessing patient medical history from their home country is essential for safe, efficient, and swift healthcare service. Access to these health records by anonymous users is not possible in the traditional authentication model.

In this work, we are presenting a Federated Identity Management System (FIDM) where every home country is able to share health records of their citizens to other hosting countries where those citizens reside [18]. This system can also be utilized within one country and among several care providers.

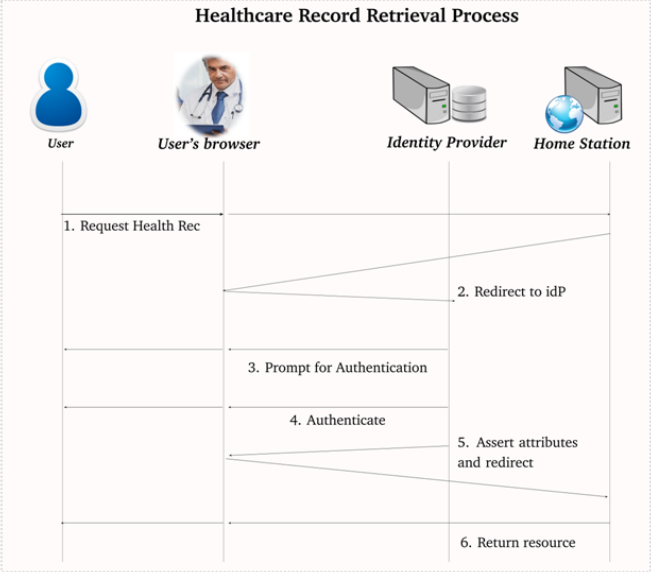

Fig. 1. Sequence Diagram for Healthcare Record Retrieval Process

Various models are suggested that provide integrity, authentication, authorization and attestation. However, each model addresses a particular aspect. A model is required which can address the aforementioned features all together. Federated Identity Management System (FIDMS) facilitates the confirmation, approval and conservation of identities. In FIDM case, a client demands a service or an asset from a Service Provider (SP). It is understood that the SP and the client don't have mutual earlier trust connection and that the SP requires some validation information to be able to provide the service. Every client might be related with at least one Identity Provider (IdP). The Identity providers can confirm the clients and give their related credentials to the SPs in view of the protection settings of the clients. These SPs give or deny access, in light of credentials and their set up (access policy as enforced by the service providers). The steps include the following: Step 1. clients submit credentials to IdP. Step 2. The privacy issues relating to a client are enforced/checked at IdP Step 3. SP trusts IdP while IdP provide clients' credentials. It is not necessary for the SP to know about the particulars of clients. It is pertinent to mention here that FIDM doesn't take into account the target's integrity. None of the current remote authentication procedures totally address the issues of security. The Identity Management Framework can be used to resolve such issues. We further incorporated trust enforced by using the blockchain infrastructure. This will be useful in addressing security issues and will measure patient's record integrity. The component layout proposed by Shibboleth is adopted for this purpose.

1) Shibboleth Project: The Shibboleth System (frequently called Shibboleth), offers a satisfactory answer for secure multi organizational access to web assets. The Shibboleth renders implementation of FIDM [18]. The versatile engineering of the Shibboleth IdP combined with its particular structure and object oriented design makes it suitable for our target design. The four principle entities that constitute the Shibboleth system are the Service Provider (SP), the Identity Provider (IdP), the customer, and the Discovery Service (DS). In a normal login situation in Shibboleth, the customer asks for the SP for an asset. In the event of a secured asset, the SP diverts the customer to the DS, which gives the customer an interface to choose their IdP.

C. Health Level Seven

Exchange of healthcare records presents a challenge to healthcare providers seeking integrated service. The Health Level Seven (HL7) is a standard that provides a comprehensive framework/structure/model for the exchange, integration, sharing, and retrieval of electronic health records of the patients [19]. The systems developed using HL7 specification, can share the medical information, such as, personal information, doctor's information, medications and healthcare records.

The author in [20] elaborates how the medical records/data from multiple sources is integrated and what is the importance of such integration in hospitals. The sharing of data among various platforms facilitate medical centers too who are attempting to find insights in the data. The HL7 has created an information system for the healthcare data known as HL7 RIM or Reference Information Model. In the research, they used HL7 RIM as an approach for the implementation of data model. Their approach, which combines elements of entity-relationship data modeling and entity-attribute-value data modeling, involves the modeling of base RIM classes, RIM inheritance, and RIM data types and incorporated the resulting data model into a way that enables medical experts to conduct clinical studies.

The customer framework inputs user's medical record, and incorporates them with HL7 message stream. HL7 messages in the customer framework transmitted over TCP/IP convention to the server framework. The server framework parses and approves this messages stream to the fragments and fields and afterward transmits affirmation to the customer framework through executing it in Java and JavaCC. The investigation of interface engine execution can be utilized genuinely in electronic wellbeing record, telemedicine framework, and medicinal data sharing among different social insurance foundations.

Our proposed global healthcare architecture is built around the concept of federated identity management (FIDM) to ensure scalability and interoperability between the service provider (i.e. the home station of the patient) and the identity provider (i.e. the healthcare provider accessing a patient's record in a given country). Typically, one of the goals of FIDMs is to ensure the privacy of the requesting entity through anonymization (by providing a delegated token). However, in our architecture, anonymization is not desired since the service provider should keep a record of all entities accessing a patient's health record. Other changes to the existing FIDM architecture are also required to fit the problem under investigation. In this section, we describe the complete architecture of the proposed system and the methodology for modifying the FIDM architecture to fit the new requirements with blockchain.

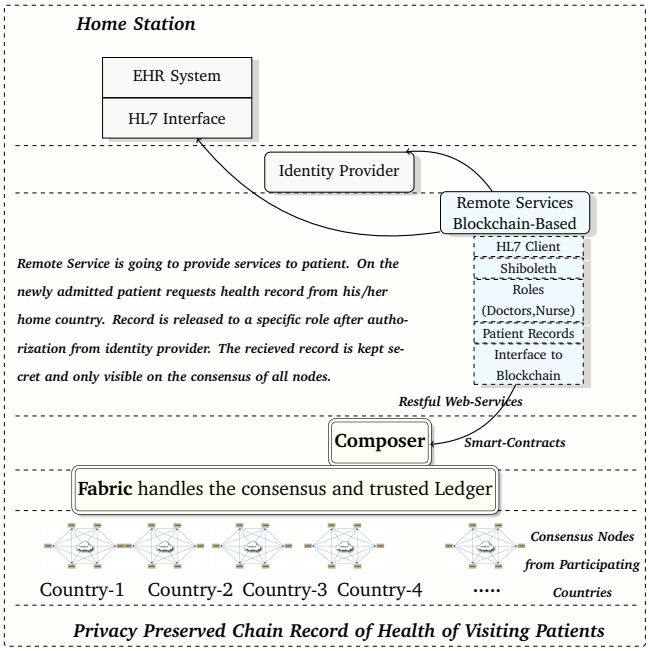

Fig. 2. Proposed Healthcare Record Sharing System

Our architecture is divided into three major modules: the service provider (SP), identity provider (IdP) and blockchain consensus/ledger. These FIDM terms are not quite applicable in the scenario addressed in this work. The service being provided to the patient is located in a remote country which requires that past health records be released by their home station. We therefore denote the patient's healthcare record provider as Home Station (HS) and the clinic in a remote country offering services to the patient as Remote Service (RS). The identity provider (IdP), however, is responsible for authentication and authorization of the healthcare record to the role(Doctor/Technician). All request and response, that is, the remote service interaction with identity provider and home station is intermediated via blockchain for integrity, privacy and consensus of all the stakeholders. Fig. 2 shows a use-case of the interaction of these entities in the proposed architecture.

When a patient visits an RS location, their healthcare records need to be retrieved from their HS. The operator at the RS opens a web page corresponding to the HS that is set up by the patient home country. The HS cannot release sensitive information to unauthorized healthcare personnel, however. Therefore, the HS redirects the browser to a login page where the operator is displayed a list of IdPs recognized by the HS. This transaction is recorded on the blockchain via blockchain intermediary node. All the communication in the remote service and server is going via the intermediary node which is further connected with blockchain interface in Hyperledger composer. A list of IdPs are provided to all the registered HS's which communicate via a signed XML document that contain (brief) metadata about registered RSs in that country. The HS redirects the request to the IdP server for authorization of the requesting role. The browser will then be redirected to the login page of the IdP. Since the HS only needs to know which of the IdPs are authorized, it does not have to know which health personnel works at a given RS, it relies to the IdP to authorize the use of sensitive resource by the operator thus making system administration feasible and scalable for the HS. After the service provider logs in to the appropriate IdP using their credentials (or using two-factor authentication such as RFIDs or biometric tokens), they are redirected to the HS along with authorization tokens released by the IdP. The HS is now able to know that the operator has been authenticated at a valid IdP. However, the exact information of the SP is not known.

While the aforementioned procedure preserves the privacy of the entities consuming given health records, it waives the right of patient to obtain knowledge about those entities. To achieve this goal, a new step is added in this workflow. After getting the authorization token (termed as auth_token) from the IdP, the HS further requests the IdP to release information about the RS requesting access to the patient's record. The IdP releases the metadata of the RS, such as, their organizational ID, their role and job description, service expiration time etc. The IdP also releases a role identifier (such as nurse, doctor, surgeon, etc.). This helps the HS decide whether to release sensitive information of the patient. This metadata is released to the HS in the form of signed XML documents encrypted through a nonce. The metadata is then digitally signed using a hashing algorithm (such as Sha256) to ensure security properties such as freshness and non-repudiation. This ensures that the same messages cannot be used by a malicious party to request the data of the patient without proper authorization, by masquerading as the RS at a later time.

After the HS validates the the metadata using the protocols associated with these security properties, it releases the patient healthcare record in a standardized format. The presented architecture adopted the Fast Healthcare Interoperability Resources (FHIR) standard (HL7) which is currently used in many countries. The use of HL7 for exchange of healthcare records ensures that minimal effort is required for integration with the proposed system

By enabling this modular architecture and distributed deployment, we aim to ease the burden of deployment for all the involved parties thus ensuring a gradual and smooth transition to the new system.

IV. Implementation

Our model is based on three modules: the HL7 client, the Shibboleth framework to provide identity management and the Blockchain for providing trusted and immutable transactions. However, interfacing directly with Hyperledger Fabric is difficult. We used Hyperledger Composer to develop the HL7 client with our permissioned blockchain network. The HL7 client requests the HL7 server, that further, authorize with an IdP. There are node.js clients available that request and parse HL7 data from the server. In our proof-of-concept implementation, we connected with the composer-client npm module to create a business network archive(BNA). When the client receives the data, it distribute the clients data in various tables of couchdb. However, each transaction is chained with blockchain network. That brings novelty in our proposed work. Each healthcare transaction is recorded and any tempering to

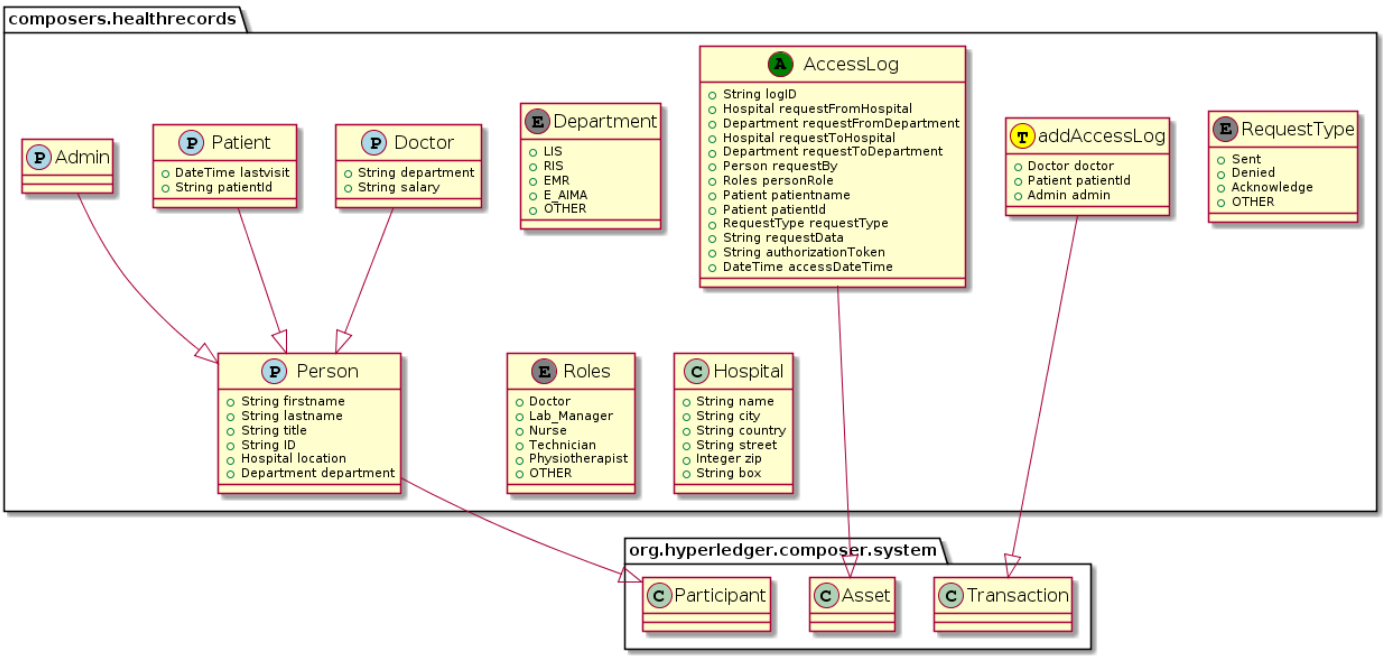

Fig. 3. BNA Data Model for the proposed blockchain section

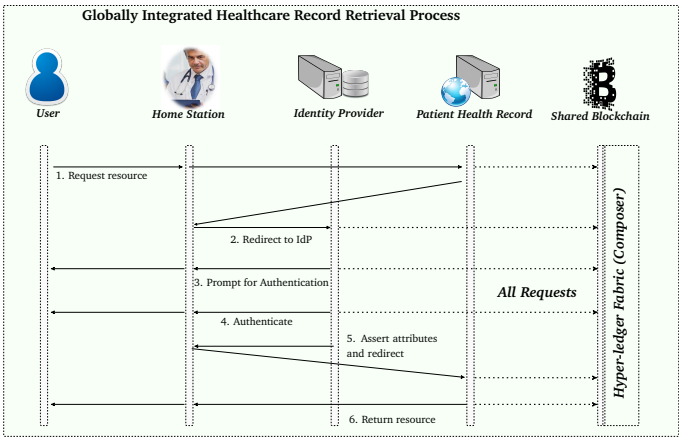

Fig. 4. Proposed Sequence Diagram for Globally Integrated Healthcare Record Retrieval Process

the records could be easily detected in database. The client, obtains the home_station information using the user's identity, such as, passport id. It then generates a request URL and communicates with the HL7 server to send/receive/parse HL7 messages.

Once the RS makes a request to the remote HL7 server for patient record extraction, it gets connected to the blockchain and the transaction is recorded. The request is then redirected to the Shibboleth module for authorization. The Shibboleth module then sends an authorization request to the HL7 client. The Shibboleth framework provides a demon process called **shibd** that runs on the Apache webserver. A web request to the Apache server is redirected to the *mod_shib*. The Shibboleth framework uses Security Assertion Markup Language *(SAML)* language to communicate between the *IdP* and *shibd*. The XML listing 1 below shows a portion of a SAML assertion containing the identity of the RS.

```
<saml:AttributeStatement>
<saml:Attribute Name="RS_client_id">
<saml:AttributeValuexsi:type="xs:anyType">
060D07777700SHZ</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="RS_id">
<saml:AttributeValue xsi:type="xs:anyType">
00DD00HHHH0F7P5</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Listing 1: SAML request for authorization from HS to identity provider

Data Provenance is a very important aspect of our model. Each transaction for a specific user for HL7 data/message manipulation is registered on the Hyperledger composer Business Network Archive model (BNA). The BNA model uses the blockchain's inherit append-only mode for recording all the transaction which are tamper-proofed. Authorized personal of a given organization can view the log on the ledger and can ensure their integrity.

In Fig. 3, the BNA Data Model deployment using Blockchain is elaborated. The model includes records related to three essential entities i.e. the participant, the asset and the transactions. A *participant* is a persons which may include the admin, a physician or a patient. Various data records are stored such as names, and departmental details their IDs and last date they had a medical checkup and which physician or healthcare clinic accessed the patient record. Similarly, to propose various health related authorized transactions to the blockchain and to represent various authorization levels for healthcare personnel different *Roles* are defined that includes limited to doctors,

lab managers, nurses, technicians, and physiotherapist. The *Asset* entity in records details of access logs pertaining various IDs. In addition, the requests made by various personnel or departments of particular hospitals regarding patient's history are also recorded. A complete workflow of our proposed solution is shown in Fig. 4.

V. Conclusion

Many reports exist in the literature regarding healthcare record sharing system. However, most of them are standalone systems serving a single hospital/clinic. Few research findings, however, discussed a unified interface for health record sharing, such as, HL7. These systems are centralized, however. Recently, decentralized systems gained popularity which revolutionized the IT infrastructure. Some solutions exist based on decentralized system, such as, blockchain. Moreover, some are healthcare record sharing systems employing an order-execute architecture known as public blockchain while some of them are execute-order architectures. The proposed solution in this research is different from the traditional healthcare record sharing system. It presents a global healthcare record extraction solution depending on the patient's location. Our proposed solution authenticate/authorize the healthcare personnel at the remote service location (providing the current medical service to patients) by utilizing the blockchain, FIDM and HL7 technologies and standards. The HL7 server is at the home_station which is located at the patient home country. Our solution shows that patients can share their healthcare records ubiquitously with various service providers. This Blockchain-based solution provides security, integrity and privacy to the patient record. All stake-holders (participating countries) are involved in the consensus process and keep copies of the health record of their home patients. Patient health records accessed by the remote service are temporary and get deleted upon patient disgorge. However, the blockchain ledger maintains an encrypted hash of that record for integrity verification and consensus process.

References

[1] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems*, vol. 48, pp. 132–150, 2015.

[2] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: state of the art and future challenges," *Journal of medical systems*, vol. 40, no. 6, p. 155, 2016.

[3] V. K. Omachonu and N. G. Einspruch, "Innovation in healthcare delivery systems: a conceptual framework," *The Innovation Journal: The Public Sector Innovation Journal*, vol. 15, no. 1, pp. 1–20, 2010.

[4] T. Viangteeravat, M. N. Anyanwu, V. R. Nagisetty, E. Kuscu, M. E. Sakauye, and D. Wu, "Clinical data integration of distributed data sources using health level seven (hl7) v3-rim mapping," *Journal of clinical bioinformatics*, vol. 1, no. 1, p. 32, 2011.

[5] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," 2016.

[6] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "Fhirchain: applying blockchain to securely and scalably share clinical data," *Computational and structural biotechnology journal*, vol. 16, pp. 267–278, 2018.

[7] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[8] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchain-based healthcare apps," *arXiv preprint arXiv:1706.03700*, 2017.

[9] A. Ekblaw, A. Azaria, J. Halamka, and A. Lippman, "A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data," *white paper*, 2016.

[10] T.-T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," *arXiv preprint arXiv:1802.01746*, 2018.

[11] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA Annual Symposium Proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[12] Z. Shae and J. J. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 1972–1980.

[13] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[14] T. Ali, M. Nauman, and S. Jan, "Trust in iot: dynamic remote attestation through efficient behavior capture," *Cluster Computing*, vol. 21, no. 1, pp. 409–421, 2018.

[15] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 2016.

[16] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017, pp. 3–7.

[17] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project," in *Blockchain enabled applications*. Springer, 2017, pp. 139–149.

[18] E. Birrell and F. B. Schneider, "Federated identity management systems: A privacy-based characterization," *IEEE security & privacy*, vol. 11, no. 5, pp. 36–48, 2013.

[19] G. J. Joyia, M. U. Akram, C. N. Akbar, and M. F. Maqsood, "Evolution of health level-7: A survey," in *Proceedings of the 2018 International Conference on Software Engineering and Information Management*. ACM, 2018, pp. 118–123.

[20] T. J. Eggebraaten, J. W. Tenner, and J. C. Dubbels, "A health-care data model based on the hl7 reference information model," *IBM Systems Journal*, vol. 46, no. 1, pp. 5–18, 2007.