A Blockchain based model for Curbing Doctors Shopping and Ensuring Provenance Management

Shekha Chenthara
Institute for Sustainable Industries and Liveable Cities
Victoria University, Melbourne, Australia
Email: shekha.chenthara@live.vu.edu.au

Hua Wang
Institute for Sustainable Industries and Liveable Cities
Victoria University, Melbourne, Australia
Email:hua.wang@vu.edu.au

Khandakar Ahmed
Institute for Sustainable Industries and Liveable Cities
Victoria University, Melbourne, Australia
Email:khandakar.ahmed@vu.edu.au

Frank Whittaker
Institute for Sustainable Industries and Liveable Cities
Victoria University, Melbourne, Australia
Email:frank.whittaker@vu.edu.au

Ke Ji
School of Information Science and Engineering
University of Jinan, Jinan, China
Email:ise_jik@ujn.edu.cn

2020 International Conference on Networking and Network Applications (NaNA) | 978-1-7281-8954-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/NANA51271.2020.00040

***Abstract*—Blockchain technology has been increasingly being recognized nowadays by healthcare industry as it guarantees precision with its secure cryptology framework and safeguards against fraud and forgery. The healthcare field is facing a major problem of Prescription Drug Abuse or Doctors shopping that entails drug misuse and leading to fatality of a large number of people worldwide. Painkillers like Oxycodone and Vicodin which are over prescribed by doctors are among the most abused legal drugs alongside sleeping pills and anxiety medication. For this reason there is an imminent need to devise a system that identifies and monitors prescription abuse. Blockchain technology's decentralisation and auditability offers a promising solution to drug tracking that not only makes prescriptions safer but also guarantees a reliable transaction history of medical records. Blockchain is one of the best ways to ensure transparency, integrity and authenticity of pharmacy or doctor's office distribution of drugs. In this research, we propose a novel drug supply chain integrity management by employing Hyperledger Fabric as the underlying blockchain platform and InterPlanetary File System (IPFS) as the decentralised file system to prevent prescription abuse. Through this approach, it is possible to recognize and track doctor's shopping and pharmacy hopping patients in an attempt to misuse drugs. The proposed system viz HealthChain solves this problem by performing drug tracking transactions by employing smart contract functionality on a blockchain to create a smart health care ecosystem. HealthChain seeks to improve the way opioid and prescriptions are administered and distributed by creating a cryptographically secure and reliable framework for physicians, pharmacists and patients.**

***Keywords*—Blockchain, Hyperledger Fabric, IPFS, Smart Contracts, Doctors Shopping**

I. Introduction

Doctor shopping is the process of visiting many physicians without professional referral to receive several prescriptions for drugs, or the medical opinion one needs to hear [1]. It has remarkable consequences for patients, as numerous consultations and overlapping prescriptions are related with drug abuse, polypharmacy, rising medical expenses and increased mortality rate. There are several explanations why patients are engaged in doctor shopping. Patients see more doctors when they have chronic disease or drug abuse and after seeking medication their health condition remains unresolved. It is a frequent practice for drug addicts, drug addiction suppliers, hypochondriacs or factitious disorder patients. These medications assist the patient in obtaining immediate pain relief, but they have also disadvantages, despite the advantages. The current prescription opioid marketplace is riddled with data hoarding, doctor shopping, provider ignorance, vulnerable, centralized data, and over-prescription. According to the

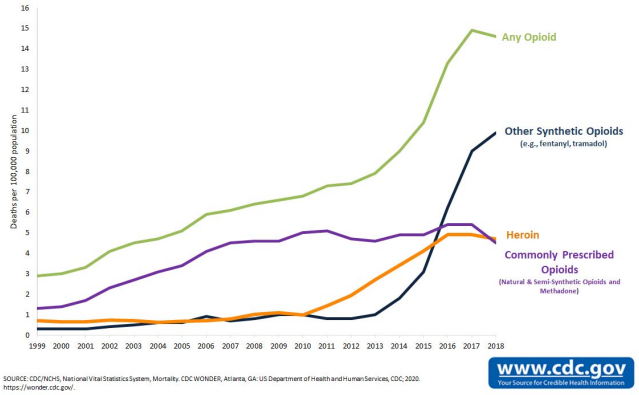

Fig. 1: Mortality rate involving opioids from 1999 to 2018

statistics, an estimated 237m drug mistakes occur annually and the expense of certainly avoidable adverse effects is calculated at £98.5 million a year, taking 181,626 bedding days, resulting in 712 deaths and 1,708 mortally wounded in NHS England [2]. Moreover, according to a study in the CURES (California's de-identified Controlled Substance Utilization

978-1-7281-8954-3/20/$31.00 ©2020 IEEE
DOI 10.1109/NaNA51271.2020.00040

Review and Evaluation System) dataset 10% random sample included 17,954,968 opioid prescriptions written by 185,424 prescribers to 3,044,579 patients with some predominated opioid [3]. Fig.1 demonstrates how opioid overdoses have increased overtime since the beginning of the epidemic. Since these opioid misuse is a challenging problem that requires a multifaceted approach, blockchain technology can help us to tackle some issues [4] [5]. Blockchain is a decentralised ledger shared by all network participants and implemented with immutability using cryptographic hash function (SHA-256) that is append-only with a time-stamped series of transactions called chain-connected blocks serves as a database of past and present transactions [6]. This data structure allows provenance which includes a single place of origin for any transaction and because all transactions are unalterable, fraudulent activity can easily be tracked. This approach curbs prescription fraud activity by making it possible to determine the quantity of medication transferred, whom medicine was transferred, when was it transferred and the frequency of patient visits.

To offset these problems with the rise of the opioid epidemic, a Blockchain-based system can set up a trusted network of hospitals and pharmacies to store opioid-related transactions including prescriptions, quantity prescribed, fulfillment, etc. in a secure and accountable manner. Also, the decentralised and distributed blockchain framework has the ability to work trustless with stakeholders by sharing an actual-time state-of-the-now database that remains in sync through consensus with immutable spate of events. The resulting immutable ledger would provide a record of drug transfers, ensure the supply chain's legitimacy and alert authorities to potentially harmful or illegal distribution patterns.

The main focus of this research is the design and implementation of a secure prescription tracking system between the provider, patient and the pharmacist on blockchain using Hyperledger Fabric as the underlying permissioned blockchain technology. Moreover, the prescription updates can be send to secure decentralized storage, IPFS after secure cryptographic encryption. We aim to establish a new drug distribution blockchain platform where electronic prescription and medication dosage, doctor and patient information are stored and exchanged efficiently across various hospital departments in a safe approved network. Moreover,this patient centric approach employs smart contracts to facilitate medical transactions and consensus mechanisms to keep the system under control in the health data network. Fig.2 shows an overview of the prescription process in the Healthchain in which the provider is facilitating a prescription and pharmacist proceeds further uploads to IPFS after secure encryption. For a controlled prescription environment, features such as patient name or id, practitioners' name or id, date of issue of the drug, drug name, drug strength, quantity prescribed, dosage form, number of refills authorized needs to be considered. The clinician prescription transactions, pharmacists updates and record updates that invoke smart contracts that creates a unique hash and adds to the healthchain. This section also discusses some of the existing techniques proposed using blockchain mechanism in healthcare management. MedRec is the first permissionless working application of healthcare that employs smart contract functionality of Ethereum to represent medical records stored in the network's individual nodes [7]. Ancile and Medrec have scalability issues which can be resolved by using

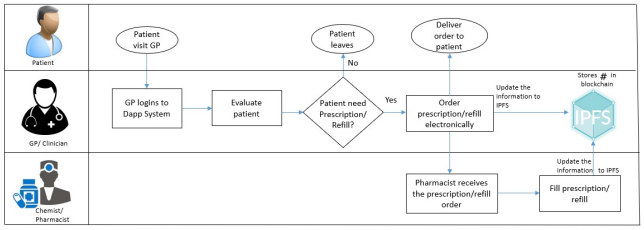

Fig. 2: Overview of medical prescription process flow in healthchain

IPFS through the secure offchain storage instead of the chains itself [8] [9] [10]. Furthermore, blockchain further extended the existing data management system for Personal Health Record (PHR) to integrate event-driven smart contracts to enable transactional services such as repeat prescription, scheduling appointments, and referral requests [11]. Sylim et.al proposed a DApp based smart contract system by employing Ethereum and Swarm as Distributed File system for surveillance in the pharmaceutical supply chain system [12]. From the detailed studies conducted and investigated by schneberk et.al [12], it is at utmost importance in surveillance of pharmaceutical drug supply chain management system to prevent prescription abuse and doctors shopping. Various security and privacy preserving solutions have been designed to protect the network against cyber attacks [13] [14] [15]. Most of the existing solutions do not guarantee the vital requirements for Elctronic Health Records (EHR), such as data privacy, security, secure storage, efficient access control, scalability and interoperability. Our research work resolves most of the existing challenges by incorporating a novel encryption technique, access control rules and smart contract functionality to demonstrate system feasibility.

The rest of the paper is organised as follows: Section II presents the architecture of the proposed framework, Section III presents implementation and simulation results and Section IV as conclusion.

II. Proposed System Architecture

Overview of the proposed system architecture is shown in Fig. 3. This represents the medical healthchain cycle with stakeholders such as Doctor, patient, pharmacist and blockchain that manages data related to drug, drug dose, prescriptions. IPFS as the offchain decentralised database for secure storage of all the health records for internal and external organisation. The hash generates by IPFS will be stored in the blockchain and the state database CouchDB which visualizes the internal blockchain structure. The Doctor can access the patient record with patients' approval and patient can also further share the health records to any authenticated Doctors in the network. The permissions can be determined by the access control rules and smart contracts in the healthchain framework. The system developed includes reliable nodes for executing a consensus protocol for distributed ledger consistency. The doctor first evaluates the patient, describes a medication, drug dosage and other advice in the form of a computerised prescription. This prescription is then sent to authenticated Pharmacist to deliver the proper medication. The

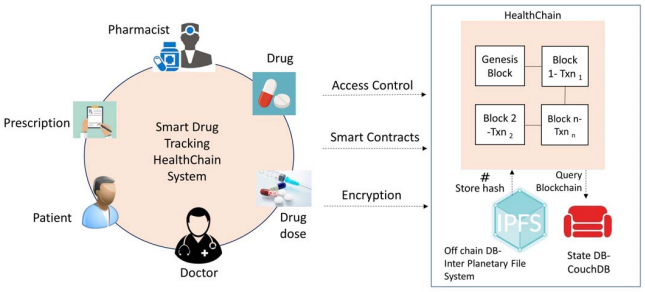

Fig. 3: System Architecture

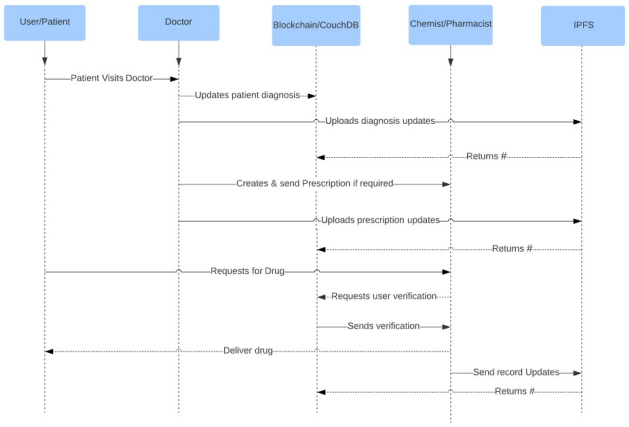

Fig. 4: Process flow in the proposed framework

Pharmacist checks the authenticity of the prescription, view the prescription, deliver the order and confirms the updates in the IPFS. The Pharmacist can only read the drug information related to the patient. The application developed is a patient-centric framework that employs smart contracts and distributed ledger as middle-ware user service. The transaction request in the proposed system is submitted by the end user (i.e. doctor, pharmacist, receptionist and patient) via the application provided by the proposed blockchain network to access back-end services such as medical prescription, profile management of stakeholders, patient appointment, EHR, EPR(electronic pharmacy record), pharmacy management, etc.

A. *Transaction flow in the proposed framework*

This prototype is designed with few stakeholders namely Doctor (Clinician), patient, receptionist and pharmacist that builts a private healthchain framework. In this proposed framework, we mainly define three entities viz Patient, Doctor and Pharmacist for interacting with the blockchain network. These entities communicate with web application via Hyperledger Fabric SDK and composer rest server API. The assets and the transactions performed will store in the couchDB i.e. the state database and this work also proposes an off-chain database IPFS that can store diagnostic documents, such as huge size images or videos [16]. The work also proposes an efficient cryptographic algorithm for storing the data in IPFS. The prescription based system works as shown in Fig.4 and the steps are as follows:

1) The framework allows the Patient to visit the authenticated Doctor and the doctor updates initial patient diagnosis in the blockchain. Doctor uploads diagnosis updates to the IPFS which returns a hash value to the blockchain database.
2) The Doctor provides the prescription after a careful examination if required, which is then added via a web application to the blockchain. The Doctor can set drug description, drug dose and even drug expiry date to prevent from further misuse by the patient.
3) The Patient requests for drug from the Pharmacist. The Pharmacist(Chemist) verifies the user, checks for prescription validity and delivers the drug for valid request else rejects the drug request.
4) The Pharmacist confirms the drug transfer and send updates to IPFS which returns a hash value for that transaction to the blockchain, thus preserves data integrity.

The working prototype is built on a permissioned blockchain called HealthChain, by combining three peer nodes to create decentralised web applications within a single organisation. This organisation has three peer nodes and an ordering node with a single public channel to register the participants in the network. A single channel has designed so that the Hyperledger Composer can communicate with the peers via the channel. Practical Byzantine Fault Tolerance(PBFT) [17] is the consensus protocol used in this blockchain based healthcare platform. Mining nodes are known as peer nodes in which the anchor peer node is chosen in a round-robin fashion from the peers. The anchor peer receives all the transactions from the network participants and validates the transactions to create a block and broadcast to all peer nodes. Each peer node Peer_i holds a copy of the ledger. The ledger can be queried via Composer rest server.

There are four stakeholders in the healthchain network H_N with n participants for each stakeholder. The Fabric-Certificate Authority issues public key certificates to all n participants such as Patient, Clinician, Receptionist and Pharmacist. There will be a key pair for each participant in which P_{Pk_i} and P_{Pr_i} as the public and private keys of the patient P_i, C_{Pk_i} and C_{Pr_i} as the public and private keys of clinician C_i , R_{Pk_i} and R_{Pr_i} as the public and private keys of the Receptionist R_i and Ph_{Pk_i} and Ph_{Pr_i} as the public and private keys of the Pharmacist Ph_i respectively where i=1 to n. The scenario in Fig. 5 gives a detailed explanation of how the Clinician, Patient and Pharmacist interacts for managing drug tracking transactions in the HealthChain framework.

The designed framework is a role-based model in which patients, physicians, chemists and receptionists can register and authenticate via client application using user credentials such as email address and password. Patient can provide appropriate read, write and deny access for EHRs to stakeholders in the network. Patient can book Doctor appointment by himself or via Receptionist. Permissioned Doctors can create medical records in the network that invokes smart contracts for committing the transaction in the network. There are several smart contracts defined in this framework for the transactions viz CreateMedicalRecord, UpdateMedicalRecord, GrantPharmacistAccess, RevokePharmacistAccess etc. All the

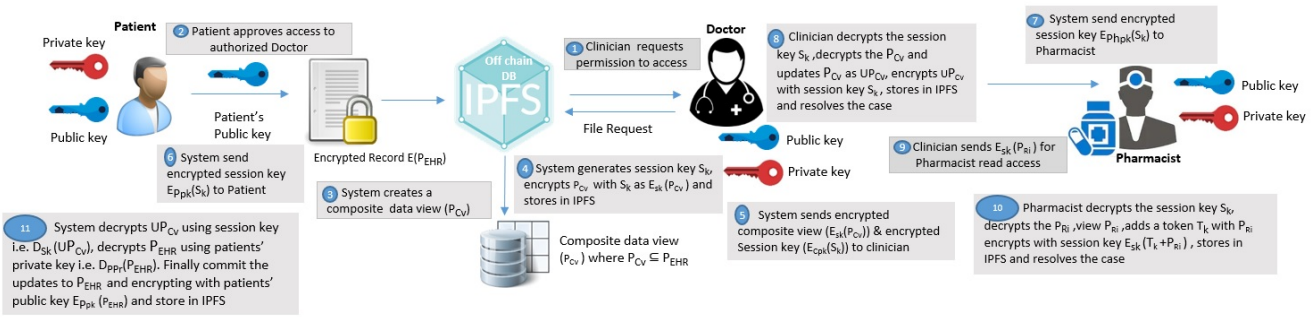

Fig. 5: Cryptographic process in the proposed framework

TABLE I: **Explanation of Notations**

Notations	Definition
H_N	Healthchain network
P_{EHR}	Patients' Health record
IPFS	InterPlanetary File System
P_{Cv}	Composite data view
S_k	Session Key
C_{Pk}	Public Key of Clinician
C_{Pr}	Private Key of Clinician
P_{Pk}	Patients' public key
P_{Pr}	Patients' private key
Ph_{Pk}	Public Key of Pharmacist
Ph_{Pr}	Private Key of Pharmacist
R_{Pk}	Public Key of Receptionist
R_{Pr}	Private Key of Receptionist
P_i	Patient
P_{ID}	Patient ID
C_i	Clinician
C_{ID}	Clinician ID
R_i	Receptionist
Ph_i	Pharmacist
Ph_{ID}	Pharmacist ID
PT_{ki}	Prescription Token
P_{Ri}	Prescription Report
UP_{Cv}	Updated Composite view
UP_{EHR}	Updated Health Record

transactions are distributed across the healthchain network in which only authenticated stakeholders can access documents which are allowed access. Each node in the framework holds a copy of the ledger and all the committed transactions are distributed across the nodes creating a decentralised network. Fig.5 illustrates the cryptographic process in the proposed framework. A detailed explanation of the cryptographic process is explained with the proposed algorithms 1,2 and 3.

B. Proposed Algorithms

This framework has four stakeholders such as Doctor, Patient, Pharmacist and Receptionist with n users for each participant. Algorithm 1 illustrates Patient working in the network, Algorithm 2 illustrates Clinician working and Algorithm 3 illustrates Pharmacist working in the healthchain network . Table I explains the notations used in the algorithm. The patient has read access to own health records and can provide read, write, revoke and deny access permissions to the authenticated stakeholders in the network. If P_{EHR_i} is not in the network, then patient provide clinician access to create P_{EHR_i}. For an existing record upon clinician request, the system creates a composite view P_{Cv_i} of the patient record P_{EHR_i}, alternately sharing the whole medical record of the patient as shown in step 15 of Algorithm 1. Composite view P_{Cv_i} is the attribute set of the stored medical record P_{EHR_i} that the system creates on permissioned user request without sharing the complete patient record. In other words P_{Cv_i} is a subset of P_{EHR_i} as shown in equation(1).

$$P_{Cv_i} \subseteq P_{EHR_i} \tag{1}$$

$$P_{Cv_i} = (D_{P_{Pr_i}}(E_{P_{Pk_i}}(P_{EHR_i}))) \tag{2}$$

$$P_{EHR_i} = [(D_{P_{Pr_i}}(E_{P_{Pk_i}}(P_{EHR_i})))+(E_{P_{Pk_i}}(U_{P_{Cv_i}})+(PT_{ki}))] \tag{3}$$

The system then creates a common session key between clinician, patient and Pharmacist for a specific session. System sends encrypted session key $E_{P_{pk_i}}(S_k)$ and composite view $E_{S_k}(P_{Cv_i})$ to the clinician. Clinician decrypts the session key with the private key and decrypts the composite view with the session key and If there are any updates, updates P_{Cv_i} as UP_{Cv_i}, resolves the case, encrypts with the session key and uploads UP_{Cv_i} to IPFS as $E_{S_k}(UP_{Cv_i})$ as shown in step 10 in Algorithm 2. if there are any prescriptions, clinician sends a prescription update P_{Ri} to the Pharmacist as shown in step 12 of Algorithm 2. Pharmacist read the prescription report and deliver the drug if the request is valid or else denies the request. Moreover, Pharmacist sends a Prescription token PT_{ki} and updates $E_{S_k}(PT_{ki})$ on placing the prescription as shown in step 7 of Algorithm 3 and resolves the case. Finally, the system commits the updates to the original record and encrypts the original record P_{EHR_i} before uploading to IPFS as shown in step 24 in Algorithm 1 and equation (3). Fig.6 illustrates the access control permission rules used in the proposed framework. Through defining the Access Control Language(ACL) rules, we can decide which users or roles in the domain model are allowed to build, read, update or delete resource components in the blockchain business network. In Fig.6 it is evident that the Chemist can read access to EHR only if the subject id matches with the resource id of the Patient.

III. Prototype Implementation and Results

We initially used a private Hyperledger fabric blockchain to implement our proposed Healthchain platform for a single organisation containing three peer nodes in a Linux environment where smart contracts are deployed for each transaction in the healthchain, IPFS storage system is used and network entities are developed to create the healthchain system. The simulation is conducted in a virtual machine environment and the PC has the following configurations.

Algorithm 1 :Algorithm on Patient working

Input: P_{ID} and P_{Pk}
Output: Get Access to Patient ledger transactions $P_L \in H_N$
Initialisation : P_L should be a valid node and can Read, Revoke, Grant or Deny EHR records

procedure Patient (P_{ID})
while (True) do
if ($P_{ID} \in H_N$) **then**
  if ($P_{EHR_i} \notin H_N$) **then**
    create_records(P_{ID}, P_{EHR_i}, H_N)
  else
    read_records(P_{ID}, P_{EHR_i}, C_{ID}, H_N)
  end if
else
  P_{ID} is invalid
end if
if visit (P_{ID} ,C_{ID}, H_N) **then**
  P_{EHR_i} = Medical_record (P_{ID})
  if ($P_{EHR_i} \in P_L(H_N)$) **then**
    $P_{CV_i} \leftarrow \int_{i=1}^{n} (D_{P_{Pr_i}}(E_{P_{Pk_i}}(P_{EHR_i})))$
    Grant_records(P_{CV_i}, C_{ID}, S_k, H_N) where $P_{Cv_i} \subseteq P_{EHR_i}$
    $C_i \leftarrow E_{C_{Pk_i}}(S_k)$
    $C_i \leftarrow E_{S_k}(P_{Cv_i})$
    Algorithm2 ()
  else
    (C_{ID}) $\leftarrow$ NOTIFY ("Medical records does not exist")
  end if
  if (UP_{Cv_i}) **then**
    $P_{EHR_i} \leftarrow [(D_{P_{Pr_i}}(E_{P_{Pk_i}}(P_{EHR_i}))) + E_{P_{Pk_i}}(UP_{Cv_i}) + E_{P_{Pk_i}}(PT_{ki})]$
  end if
  if ($P_{EHR_i} \in C_{ID}$, treatment completed (P_{ID})) **then**
    end session (S_k, P_{EHR_i}, C_{ID})
  else
    (C_{ID}) $\leftarrow$ NOTIFY ("voluntary revoke P_{EHR_i}")
    Revoke_records(P_{EHR_i}, C_{ID}, H_N)
  end if
else
  Not visit
end if
end while
end procedure

Algorithm 2 :Algorithm on Clinician working

Input: C_{ID} and C_{Pk}
Output: Get Access to Clinician ledger transactions $C_L \in H_N$
Initialisation : C_L should be a valid node and can Read or Write EHR records permissioned by the patient

procedure Clinician (C_{ID})
while (True) do
if ($C_{ID} \in H_N$) **then**
  if (Granted P_{EHR_i}) **then**
    Read_records(C_{ID}, P_{EHR_i}, H_N)
    Update_records (C_{ID}, UP_{Cv_i}, H_N)
    $C_i \leftarrow D_{C_{Pr_i}}(S_k)$
    $C_i \leftarrow D_{S_k}(P_{Cv_i})$
    $P_{Cv_i} \rightarrow (UP_{Cv_i})$
    IPFS $\leftarrow E_{S_k}$ (UP_{Cv_i})
  end if
  Pharmacist $\leftarrow P_{Ri}$
  Algorithm3 ()
else
  C_{ID} is invalid
end if
end while
end procedure

Algorithm 3 :Algorithm on Pharmacist working

Input: Ph_{ID} and Ph_{Pk}
Output: Update Prescription confirmation to Patient Ledger transactions $P_L \in H_N$
Initialisation : Ph_{ID} should be valid and can Read Prescription records permissioned by the Clinician

procedure Pharmacist (Ph_{ID})
while (True) do
if ($Ph_{ID} \in H_N$) **then**
  if (Granted P_{Ri}) **then**
    Read_records(Ph_{ID}, P_{Ri}, H_N)
    Pharmacist $\rightarrow$ (PT_{ki})
    IPFS $\leftarrow E_{S_k}$ (PT_{ki})
  end if
  Algorithm1 ()
else
  Ph_{ID} is invalid
end if
end while
end procedure

- Ubuntu Linux 16.04 LTS 64 bit
- 2 Core CPU (Intel Core i5 2.5GHz (Turbo Boost up to 2.7GHz) with 3MB shared L3 cache
- 5GB Memory
- 1 Gbit/s network
- 30GB SSD

Fig.7 shows the illustration of creating prescription in Doctor's profile in the healthchain framework. Furthermore, this system also allows a patient to view the medical records and also keeps a provenance history of the medical records.

Fig.8 portrays querying of the records via Composer Rest Server API in the proposed system and Fig.9 shows the scalability of storing health records in IPFS. IPFS stores the records in different nodes if the size greater than a particular threshold (greater than 256KB). For this research, the records will be stored in a way to make it cryptographically protected after encryption with the specified encryption algorithm. Fig.9 shows the uploading and downloading time of 5 concurrent users in the healthchain network. Considering the system requirements, the system took an average of 60 seconds to upload the data to IPFS and 80 seconds to download a 100MB data from IPFS. This research adheres improved security with the proposed encryption, improved privacy with the defined access control rules, enhanced integrity with the proposed blockchain framework and improved scalability with the introduction of IPFS for a decentralised data storage.

/* Access control rules for EHR-network*/

- rule DoctorCanReadPatient {
  description: "Allow doctor read access to all granted patients"
  participant(p): "org.ehr.healthchain.Doctor"
  operation: READ
  resource(r): "org.ehr.healthchain.Patient"
  condition: (r.authorized && r.authorized.indexOf(r.getIdentifier())>-1)
  action: ALLOW }
- rule DoctorCanUpdateEHR {
  description: "Allow doctor update access to all granted patients"
  participant(p): "org.ehr.healthchain.Doctor"
  operation: CREATE,UPDATE
  resource(r): "org.ehr.healthchain.Patient"
  transaction(tx):"org.ehr.healthchain.UpdateRecord"
  condition: (r.authorized && r.authorized.indexOf(p.getIdentifier())>-1)
  action: ALLOW }
- rule ChemistCanReadEHR {
  description: "Allow chemist read access to all granted patient records"
  participant(p): "org.ehr.healthchain.Chemist"
  operation: READ
  resource(r): "org.ehr.healthchain.Medical_Record"
  condition: (ph.ChemistId == r.PatientId)
  action: ALLOW }
- rule DoctorCanUpdatePatientPrescriptionDose {
  description: "Allow doctor update access to all granted patients"
  participant(p): "org.ehr.healthchain.Doctor"
  operation: READ, CREATE, UPDATE
  resource(r): "org.ehr.healthchain.UpdateMedical_Record"
  condition: (r.authorized && r.authorized.indexOf(p.getIdentifier())>-1)
  action: ALLOW }

Fig. 6: Access permission rules in the proposed framework

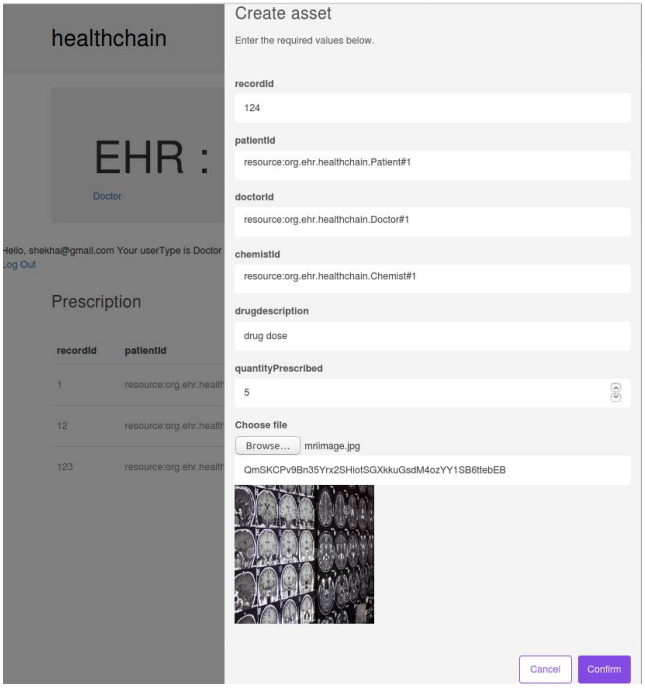

Fig. 7: Illustration of EHR Prescription creation in Doctor's profile in the proposed HealthChain

Several experiments were executed to perform Transaction Latency of the proposed framework. Transaction latency is the time needed to commit the transaction and is available across the network nodes. Transactions defined are: (a)Create Medical Records (b)Update Medical Records (c)Update Ownership (g)

Fig. 8: Illustration of querying the health records in the proposed HealthChain

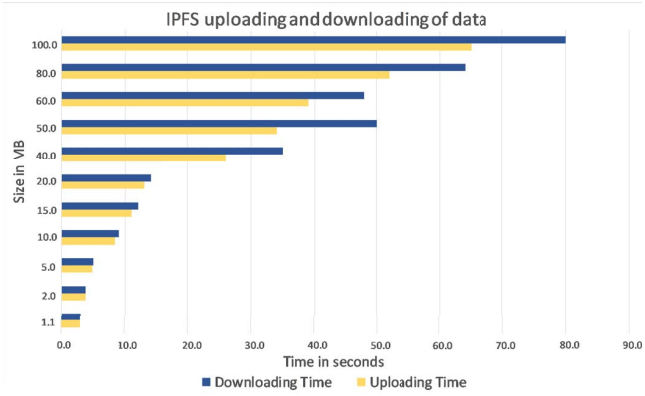

Fig. 9: Scalability in IPFS

Prescription to Pharmacist used in this experiment. if there are n number of nodes in the blockchain network in which T_{L_n} is the Transaction Latency and the confirmation time is T_{C_n} in the network nodes and transaction submit time in seconds is T_{S_n} then;

$$T_{L_n} = T_{C_n} - T_{S_n} \tag{4}$$

The experiments have been executed in three peer nodes with seven sets of transaction commit to the network ledger in varying size transaction sets of 5, 10, 15, 20, 30, 40 and 50 as shown in Fig.10. Considering the machine configuration, it is evident that the first 5 set of transactions took an average of 80 seconds to commit, second 10 set of transactions took an average of 97 seconds to commit and the last set of 50 transactions took an average of 160 seconds to commit across the network. It is therefore apparent that with an increase in

peers and an increase in the number of transactions, the time required to execute transactions increases.

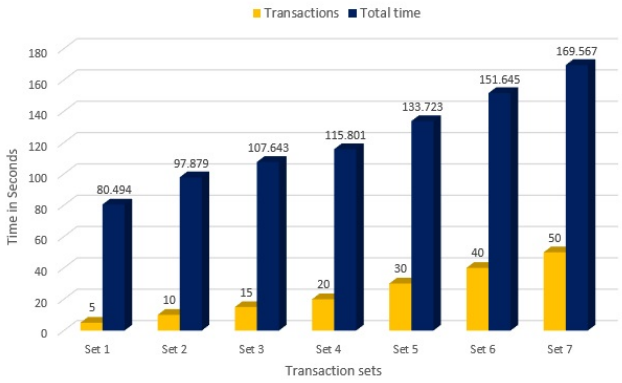

Fig. 10: Transaction Latency

IV. Conclusion

In this research work, a permissioned Blockchain framework has been implemented for secure drug prescription tracking between stakeholders in healthcare utilizing Hyperledger fabric and Hyperledger composer. This work created smart contracts for various medical work flows, and then data access permissions are managed by patient in the healthcare ecosystem. Moreover, this research proposes an efficient cryptographic mechanism for securing data storage and providing efficient access control between stakeholders viz patients, doctors, pharmacists and other participants via encryption techniques and access control mechanisms. A working prototype based on Hyperledger Fabric and Interplanetary File System are made to illustrate the system's viability and consequently, the framework is successful as a reliable health data network. With healthcare data growing each year, we look forward to improving this prototype with robust scalability simulations and comparing it with other blockchain architectures in a test bed arena that invites more interest in future research work.

References

[1] M. Biernikiewicz, V. Taieb, and M. Toumi, "Characteristics of doctor-shoppers: a systematic literature review," *Journal of market access & health policy*, vol. 7, no. 1, p. 1595953, 2019.

[2] D. Dowell, K. Zhang, R. K. Noonan, and J. M. Hockenberry, "Mandatory provider review and pain clinic laws reduce the amounts of opioids prescribed and overdose death rates," *Health Affairs*, vol. 35, no. 10, pp. 1876–1883, 2016.

[3] T. Schneberk, B. Raffetto, J. Friedman, A. Wilson, D. Kim, and D. L. Schriger, "Opioid prescription patterns among patients who doctor shop; implications for providers," *Plos one*, vol. 15, no. 5, p. e0232533, 2020.

[4] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-health solutions in cloud computing," *IEEE access*, vol. 7, pp. 74 361–74 382, 2019.

[5] H. Wang, Z. Zhang, and T. Taleb, "Special issue on security and privacy of iot," *World Wide Web*, vol. 21, no. 1, pp. 1–6, 2018.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[7] C. Dannen, *Introducing Ethereum and Solidity*. Springer, 2017.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016.

[9] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018.

[10] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[11] G. Leeming, J. Cunningham, and J. Ainsworth, "A ledger of me: personalizing healthcare using blockchain technology," *Frontiers in medicine*, vol. 6, 2019.

[12] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention," *JMIR research protocols*, vol. 7, 2018.

[13] H. Wang, Y. Wang, T. Taleb, and X. Jiang, "Special issue on security and privacy in network computing," *World Wide Web*, vol. 23, no. 2, pp. 951–957, 2020.

[14] H. Wang, X. Yi, E. Bertino, and L. Sun, "Protecting outsourced data in cloud computing through access management," *Concurrency and computation: Practice and Experience*, vol. 28, no. 3, pp. 600–615, 2016.

[15] M. Li, X. Sun, H. Wang, Y. Zhang, and J. Zhang, "Privacy-aware access control with trust management in web service," *World Wide Web*, vol. 14, no. 4, pp. 407–430, 2011.

[16] J. C. Anderson, J. Lehnardt, and N. Slater, *CouchDB: the definitive guide: time to relax*. " O'Reilly Media, Inc.", 2010.

[17] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018.