2020 Seventh International Conference on Software Defined Systems (SDS)

Health Care Insurance Fraud Detection Using Blockchain

Gokay Saldamli*, Vamshi Reddy*, Krishna S. Bojja*, Manjunatha K. Gururaja*, Yashaswi Doddaveerappa*, Loai Tawalbeh§
*Computer Engineering Department
San Jose State University
San Jose, CA, USA
Email: gokay.saldamli@sjsu.edu
§Dept. of Computing and Cyber Security
Texas A&M Univ. - San Antonio
San Antonio, TX, USA

***Abstract*— The health care industry is one of the important service providers that improves people lives. As the cost of the healthcare service increases, health insurance becomes the only way to get quality service in case of an accident or a major illness. As health insurance will reduces the costs and provides financial and economic stability for an individual. One of the main tasks of healthcare insurance providers is to monitor and manage the data and to provide support to customers. Due to regulations and business secrecy, insurance companies do not share the patient's data but since the data are not integrated and not in sync between insurance providers, there has been an increase in the number of fraud's occurring in healthcare. Often times ambiguous or false information is provided to health insurance companies in order to make them pay for some false claims to the policy holders. The individual policyholder may also claim benefits from multiple insurance providers. There is a financial loss of billions of dollars each year as estimated by the National Health Care Anti-Fraud Association (NHCAA). In order to prevent health insurance fraud, it is necessary to build a system to securely manage and monitor insurance activities by integrating data from all the insurance companies. As blockchain provides an immutable data maintaining and sharing, we propose a blockchain based solution for health insurance fraud detection.**

Keywords*— Blockchain, Healthcare, Ethereum, fraud detection.

I. INTRODUCTION

Healthcare data is attracting the attention of many cyber-attacks since the internet has revolutionized [1]. Although there have been many architectures and protocols established to secure health care data and providing approaches to prove their validity, hackers still seem to find a way to get through them. According to HIPPA journal, there have been 77 breaches of health care data within the first three months of the year 2018 which resulted in data leak of more than a million records. Although the number of breaches has been decreasing over the year, the severity of the breach effect has been multiplying. Also, having a central authority over a database containing healthcare data can be a major security threat. This calls for a system to securely manage and store healthcare data.

Blockchain gained popularity over the years and its interest in the healthcare industry resulted in design principles to alleviate security problems [2]. Since Blockchain offers decentralized distributed paradigm, this work leverages Blockchain technology to mitigate the problems posed from attackers and making transactions and logging of data more secure. There would be companies grouping up to collaborate and share medical records. This assures the shared medical records are visible to only the parties involved in the chain. We utilize Ethereum's smart contracts to create intelligent representations of existing medical records that are stored within individual nodes on the network [3]. Some of the Application of block chain-powered smart healthcare include fast Healthcare Interoperability Resources, User-Oriented Medical Research, Counterfeit Drug prevention and Detection [4]. NHCAA has provided the list of frauds scenarios that are observed in healthcare insurance claims which cost billions of dollars of loss to healthcare insurance providers. In this work, we are implementing the distributed network using Blockchain to find few scenarios of the fraud insurance claims. TO be specific, we want to tackle the two most fraud scenarios observed as mentioned below.

- Theft of Patients Finite Health Insurance Benefits where an individual's health insurance benefits will be stolen.
- Usage of multiple insurances to have additional profit.

In this work, we defined a conceptual model in which primarily, the misleading information are removed by following a set of rules called HIPAA Privacy rules defined by US Department of Health and Human services to securely maintain health-related information of each individual in the country. Further, insurance fraud can be prevented by leveraging Blockchain technology to permanently log all transactions of policyholders. By use of security features available on the block-chain, we have provided access only to the particular parties to

978-1-7281-7219-4/20/$31.00 ©2020 IEEE

access the data. Blockchain assures that each block of data is visible to all parties involved in the chain by removing the need of a third party. Companies grouping up together to share data in Blockchain would result in less manipulation in policies. We have integrated and linked information about the claimer from various health insurance companies using Blockchain technology and is used as a reference to detect fraud. This method can mitigate health insurance fraud by offering transparency not present in the current paradigm of the health insurance world. Hence by allowing all the parties in the Blockchain to view the patient's records and make sure the data is accurate before sanctioning of the insurance to the customer.

II. Problem Statement

The healthcare industry is constantly reforming and adopting new shapes with respect to technological evolutions and transition[5]. It is necessary to maintain and monitor the patient's record without any ambiguity. Quality healthcare services have to be provided to users. Because of the growing technology, it is necessary to build a system in which the data is secured and maintained accurately. Due to the lack of traceability in the data transaction and the records, there have been several problems in the healthcare system.

The healthcare insurance companies are using an outdated method to keep track of the health care records and the insurance approved details of the customers. This makes a way for many frauds to occur in the health insurance domain. The customer tries to claim for the insurance at two different parties, by cheating the insurance companies. Hence it is very necessary to build a secure system and keep track of all the claimed insurance from a user so that the fraud can be detected. Accordingly, the number of fraud occurring in healthcare can be reduced and more appropriate quality services can be provided to the users.

This requires a need to build a system, that removes middlemen and make use of technology to store and trace the data. The solution is to make use of the Blockchain technology, which helps in data integrity and security. The data once written on a Blockchain cannot be modified or deleted, this feature of Blockchain provides data integrity in detecting fraud. If any changes are made to the node on the block-chain, then all subsequent changes have to be made on the other nodes. Blockchain also keeps track of the log activities, which allows the admins to access anytime. Even though there are certain limitations in regards to Blockchain technology, it is one of the most popular techniques used today in the healthcare sector. Therefore Blockchain helps us to overcome many of the challenges that exist in the healthcare industry including data integrity, data security, and fraud detection.

III. Architecture

The prototype we built consists of a frontend, backend and database using the following technologies:

- React.js and Redux for front end application development, Flask and BigchainDB for backend development.
- EDI Validator to check the validation of the insurance records before uploading into blockchain and REST API calls for communication between the client and server.
- Deploying the application on a blockchain, so it will be available to users all the time.
- Security is the main goal in the digital world. We are ensuring that the security of the system is not compromised. Personal data theft is one of the major growing concern today.
- Neo4j a graph database used for fraud detection, graph-based search and time tree model for analytics. Neo4j offers three ways to query, and evaluate its query performance from several dimensions: data size, query complexity, query number, etc. [6].

The backend is developed using Flask framework and we have used BigchainDB (MongoDB) and Neo4J (Graph Database) as a Database.

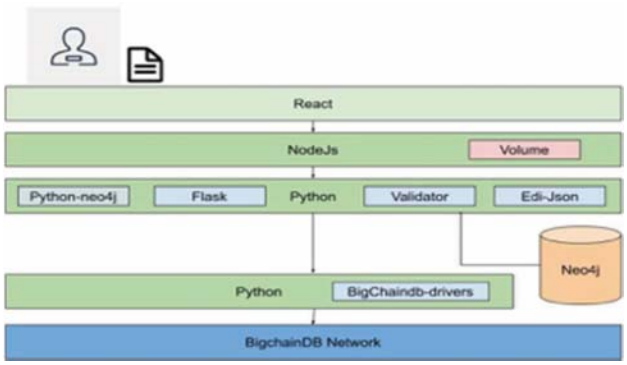

Fig. 1. High-level architecture

Fig. 1 is the design architecture of our system. It follows MVC architecture. Users interact with the system using web application. The backend server is developed on Python Flask framework and MongoDB database to store user details, login credentials, and access control list. User uploads the Insurance claim document to the system. The user is alerted with the error message if the EDI Validation process fails. The document is shared on the blockchain if the validation is successful and is available to all the users.

Since we don't have an update option in blockchain, we must verify the correctness of the data before writing. For this reason, we have used an additional step called EDI Validator. It is also used to verify if the data follows HIPPA Guidelines. File EDI 837 contains the details about the claim request raised by the patient and File 835 contains the Payment information for medical service. Health Care Insurance providers have to follow HIPPA 837 Professional health care guidelines additional to the standard 837 Electronic data interchange rules. Level 6 and Level 7 of EDI validation will check specific health care providers business rules. All providers will use and accept standard rules of 837 transactions from Level 1 to level5. General procedure for electronic claims submission: A submitted 837 claims file is either accepted or rejected if it contains any invalid data. We basically check whether the loops, segments and data elements in the file are following the rules from the HIPAA 837 report. They have to use proper data separators (delimiters) at the right place, and also avoid the usage of delimiters inside the data content.

All the transactions are validated, "997 Functional Acknowledgement – Reject" is sent to the provider in case of validation failure and the user is expected to correct the file content and upload again. Health care providers follow certain guidelines to store health care records. These rules are set by EDI electronic data interchange. Data is grouped based on its type. Provider name, Patient name, Hospital Address, Type of service, Health Care plan user has enrolled, claim amount requested by the client.

We have generated an XML tree from the data. It will tell us if a required segment is missing. Each segment has a segment header. Segment header will tell us what type of data the segment holds. EDI has its own syntax or data representation standard. Like colon at the end of every line for all statements in C programming. Same way here we separate each segment by and separate elements in a segment by *.

A. *Frontend*

React with Redux is used to develop User Interface, Login, Signup and File drop.

B. *BigchainDB*

We have used BigchainDB to store healthcare records in a distributed database. Using this we can manage all insurance companies data. We maintained all the claim and payment data. Client has to provide claim id to check their claim status. We use EDI 835 payments data, to know the status of a particular claim and update the database. It provides high security and privacy for data.

C. *Microservices*

We have used flask framework to develop our back-end micro-services. The reason behind using nodejs is that, it is an asynchronous API. Nodejs improve speed and efficiency. It is light weighted and easy to use a framework.

D. *Authentication*

1) We store the hash value of the password in the database. When user tries to login we generate hash for user entered password and compare it with the database hash, if both the hash values match then we Authenticate him as valid user.

2) We send a confirmation link to the registered email address after signup, the user has to click on that link to activate his account within 24 hours.

3) We send a unique session key to every user each time they log into the application.

E. *Cloud deployment*

Graph databases provide an effective way of storing and relating data. A proper model in a graph database can be used for various purposes, one of which is fraud detection. There is lot of capital losses for banks and insurance companies to fraud every year. There are many complicated systems built to reduce them. But no technology can completely evade the losses to fraud.

Graph database presents a solution to detect advanced fraud scenarios in the real time. In health care, medical records hold a lot of details apart from that of patient, like hospital in which the treatment has been issued, reason for visit, date, procedural treatment that is provided, doctors in charge, facility code, discharge date, etc. By storing all the data in graph database and creating a well-structured model forming relations between relevant data can lead to a system that can be used to detect fraud.

Neo4j, one of the lead graph databases, provides a simple way of achieving this model. The retrieval of the data is much faster compared to traditional relational databases. Complex queries can be performed with simple statements called cypher. We can also find significant insights by rephrasing problem in simple terms. We have created Docker image for the nodejs, python, neo4j and react to reduce dependency, to provide isolation and standardization. We have hosted our application on AWS.

IV. SYSTEM DESIGN

BigchainDB, an open source technology is used to create a distributed database on blockchain concepts. MongoDB database is used to store the blocks in each node of BigchainDB, since it provides better consistency of records compared to other kinds of databases that are supported by BigchainDB.

The flask, NodeJS backend server is setup on AWS. The raw Healthcare Records used in the initial evaluation are from Medicare – Lumeris. A React-Nodejs application is used to upload raw medical records in user interface. This file is stored in a location which is accessible by a flask application.

A REST call is sent from NodeJS to flask application specifying the filename and other details. The flask application picks up the file from a designated folder and run a custom validation function that validates the authenticity of the medical data. After it has been successfully validated, it will generate an intermediary JSON. This Json in-turn loaded to neo4j(graph database). Graph database is used to load data hierarchically and for faster retrieval of results. Neo4j is queried for specific details and an object containing these details are sent to client application that interfaces with blockchain.

The client application deserializes the object and commits a transaction containing these details into BigChainDB which is backed by MongoDB.

Fig. 2. sample EDI data in Neo4J

As the files are being added, it is very important to keep the record of when they were uploaded. And some nodes within 837 transaction files also represents time instance like the date-time at which the transaction took place or DOB. All these nodes containing timestamps can be linked to another graph called Time-Tree. This could ease the retrieval of files based on the time that they were uploaded. The timestamp nodes are automatically connected to the Time-Tree graph as they get uploaded. REST API is also provided to retrieve these events. Only the files that cleared all the validations are stored and others are sent back as a message to the loading system. After certain processing of data in the neo4j database like data modification and validations, the files will be finally transferred to MongoDB, which is NO-SQL database. This database has a well-defined API to connect to the blockchain data structure.

V. IMPLEMENTATION

The implementation is divided into 4 phases. The first phase consists of developing backend services which will validate 837 files, process https client requests and manage data with the blockchain securely. In the second phase, neo4j is used to perform level 4 - level 7 HIPAA validation. It is also used to store other essential metrics such as logging. In the third phase, we develop the user interface and additional security measures. In the fourth phase, we will deploy the servers in the AWS.

A. First Phase

We have gathered necessary standard EDI 837 claims rules, getting these details from internet and Medicare official website and gathered 837 files from Lumeris Inc. Level 1 deals with syntax errors, segment order, element attributes. Level 2 deals with loop count, recommended vs not recommended segments/elements, valid code values, HL parent/child relationship. Level 3 deals with balance validation. Level 4 deals with situational requirement testing.

To achieve performance, we run 4 threads in parallel, one thread for each level of validation. If we found any errors in the data representation, we store them in the error message and return it back to the user. After the validations are passed, the results are dumped backed to neo4j database. After we receive the file, we trigger the validation service. Validation service will take the filename as input. It checks if the health care records in the file satisfy all the EEDI HIPAA rules. We validate it against Level 1 to Level 5. If there are any errors we notify the user in the validation dashboard. We are developing multiple rest API's to offer the service to customers.

B. Second phase

To have built the blockchain distributed system in AWS and used BigchainDB, an open source technology available to create a distributed database on blockchain concepts.

In this distributed database, the insurance companies will be participants and each insurance company will be provided with a BigchainDB node. In our study, the user healthcare insurance claim information will be considered as assets. So each insurance company will be able to perform only Create Transaction, to create the assets and store it in the Blockchain system and there will be no scenarios to perform Transfer Transaction. To create the transactions for assets in the blockchain, the BigChainDB has provided the drivers in multiple languages.

BigchainDB server uses Tendermint software for consensus and for secure replication of records across nodes in the Blockchain network. Tendermint implements Byzantine fault tolerance principle(BFT). As per the Tendering official documentation, "The ability to tolerate machines failing in arbitrary ways, including becoming malicious" is known as Byzantine fault tolerance.[6] Tendermint consists of 2 components, Tendermint core, which is a consensus engine module and the other one is Application BlockChainDB Interface (ABCI), which enables to handle the transactions in any programming languages.

To store the blocks in each node of BigchainDB, we have used MongoDB database. The BigchainDB supports other databases as well, such as Postgres database, RethinkDB database, etc. But for the application that we are going to build on the top blockchain network, MongoDB provides better terms of consistency of records compared to other kinds of databases that are supported by BigchainDB.

We have unique billing id for each service that a client takes in clinic, lab or pharmacy. The patient can raise the claim for a particular service by providing their billing id and patient id. Before approving a claim, we need to check the payment(835) data for the corresponding billing id. Now for each billing id the claims file we check if there are any previous payments approved with the same billing id. If the billing id is not present in the 835 we process the payment and update the 835. We then insert the 835 and 837 files data into the blockchain. If there is a negative balance, it means something wrong with the claim request. There might be a chance for fraud.

C. Third phase

We have developed web user interface for our application and is being used by healthcare professionals. A secured (SSH) tunnel to transfer data between frontend and backend.

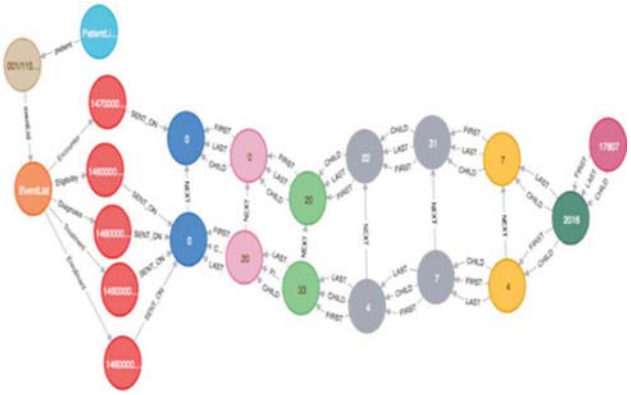

Fig. 3. Time series model for logging

A graph model in neo4j is developed to store and visualize all events that a patient has gone through. All the events are given a timestamp which details when they occurred. The accuracy of the timestamp is down to milliseconds.

D. *Fourth phase*

We have deployed our environment on AWS, which will be running continuously to service all the incoming requests. We have used Blockchain, to provide default security to the data in it. Encrypt the healthcare records using a private key and store it on the BigchainDB database. Since records are stored at multiple nodes, we have ensured reliability from the blockchain. Blockchain ensures consistency and availability.

VI. Evaluation Methodology

To have built blockchain distributed system in AWS and used BigChainDB, an open source technology available to create a distributed database on blockchain concepts. MongoDB database is used to store the blocks in each node of BigchainDB. The BigchainDB supports other databases as well, such as Postgres database, RethinkDB database, etc. But for the application that we are going to build on the top blockchain network, MongoDB provides better terms of consistency of records compared to other kinds of databases that are supported by BigchainDB.

The flask backend server is setup on AWS. Once the web interface is finished, access to the server is available as a REST API. The raw Healthcare Records used in the initial evaluation are from Medicare - Lumeris. The level 1 HIPAA validation has been performed using scripts written in python. The validations were successful, yielding filtered data that can be passed to the level 2 HIPAA validation. All the level 1 validated healthcare records are converted from their raw form into structured JSON format. This conversion is done considering 837 claim conventions. The JSON contains pairs, where keys resemble names of what values represent. Storing the initial data in JSON provides an efficient way of accessing information and in turn, makes it easy to load them into other databases.

Sample JSON records are loaded into the Neo4j graph database where HIPAA level 4 - level 7 validations can be performed. Modeled a systematic graph structure to effectively access data. Retrieving information stored in the graph database is proved to be 50% faster than traditional relational databases.

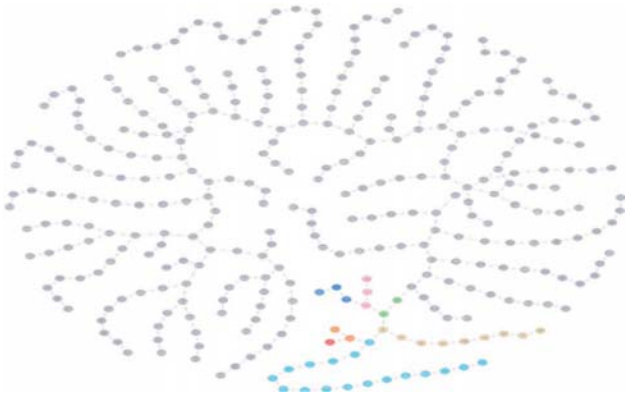

Fig. 4. Healthcare record in Neo4j graph database

Fraud detection and HIPAA validation system should be tested to see if the application is running continuously and to check the proper functioning of the blockchain system with and without the delayed timestamp validation algorithm.

As we progress, various types of testing are done:

1) Unit Test - A python module named Unit test is used to perform a unit test. All the functions written in python are tested for accuracy and to check whether all corner cases are met.
2) Integration Test - Mocha is used to test multiple functions that passed a unit test to assure that these functions work together.
3) System Test - This test is performed to check whether the system as a whole behaves as desired. The system can be mock tested after all the components like the python flask service, HIPAA validator, blockchain, database modules have been integrated.
4) Smoke and Regression Test - Regression testing is performed when the development environment changes, this makes sure that lack or mismatch of dependencies doesn't affect the behavior of the prototype.
5) Performance Test - Apache JMeter is used to find the latency of the server.

VII. Related Work

It is believed that around 16% of the United States GDP is spent on Health care, out of which significant amount of resources are wasted because of Medical Errors, Fraud and Abuse, payment for services which are not delivered [6]. It is estimated that there is around 3% to 10% of health insurance claims are a fraud and this condition is similar in most of the countries around the world [7]. According to the National Healthcare Anti-Fraud Association (NHCAA), there will be around tens of billions of dollars of loss caused by health insurance fraud cases each year. The NHCAA has provided a list of fraud cases which includes False Patient Diagnoses, Treatment and Medical Histories, Theft of Patients' Finite Health Insurance Benefits, claiming insurance from multiple insurance companies, etc. [8].

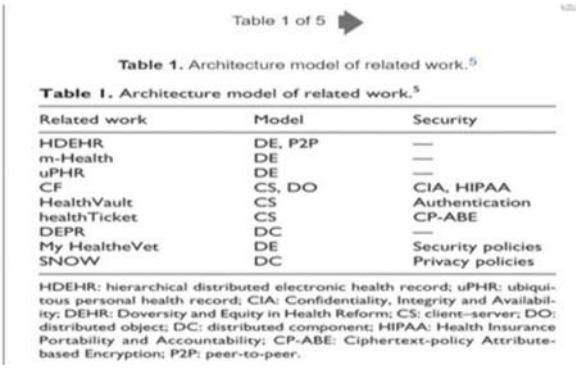

Table 1 of 5

Table 1. Architecture model of related work.[5]

Table 1. Architecture model of related work.[5]

Related work	Model	Security
HDEHR	DE, P2P	—
m-Health	DE	—
uPHR	DE	—
CF	CS, DO	CIA, HIPAA
HealthVault	CS	Authentication
healthTicket	CS	CP-ABE
DEPR	DC	—
My HealtheVet	DE	Security policies
SNOW	DC	Privacy policies

HDEHR: hierarchical distributed electronic health record; uPHR: ubiquitous personal health record; CIA: Confidentiality, Integrity and Availability; DEHR: Doversity and Equity in Health Reform; CS: client–server; DO: distributed object; DC: distributed component; HIPAA: Health Insurance Portability and Accountability; CP-ABE: Ciphertext-policy Attribute-based Encryption; P2P: peer-to-peer.

Fig. 5. Security of different health record databases

In Fig. 5 the models concentrate on health data of all patients in single and multiple servers, following a centralized client-

server (CS: client-server, DO: distributed object, DC: distributed component, DE: distributed event-based).

Many approaches are available to detect health care fraud claims in Machine learning and big data fields. One of the proposed methods available to find fraud detection in health care insurance claim by data-driven method on the comparative research, fraud cases and literature review[9]. It is believed that there will be a possibility of not noticing the fraud cases using SQL operation on a large cluster of databases using heuristic rules. The authors in [8] used clustering methods such as SAS EM and CLUTO to detect the fraudulent in insurance claims for the clustered high volume of databases. Big data analytics techniques can also be used fully in finding the fraud detections and to provide better health care services [10].

In this study, we use the Blockchain Technology to find fraud insurance claims in the Healthcare industry. Blockchain technology ”provides easier, quicker, more efficient, and more secure sharing and exchange of data, information, and funds in assorted ways” [11]. A ledger of a record will be maintained in synchronization with all the nodes involved in the distributed system which does not affect the failure of one system on the distributed network.

Although, Blockchain as a technology was originally designed for Bitcoin cryptocurrency, it has been found to be useful in a wide range of applications such as energy sector, smart contracts, personal data protection, healthcare and intelligent transportation systems [12]. Blockchain technology provides the security for a distributed system which involves the transactions of information between the nodes in the system [13]. The blockchain technology developed on the distributed databases prevents tampering, malicious misuse of the health records and maintains the log of all operations performed on the data in the database [14].

The blockchain technology is not just limited to the finance field and it is also adopted to IOT field for more reliable data transfer between the IOT devices [15]. Patients Healthcare records are very confidential and should be stored in a secure way. In order to protect the data, various mechanisms were introduced such as numerous authentication scheme [16]. These schemes were helpful to some extent to provide security for the data, but due to improvement in the technology, these approaches are not just sufficient because the patient has been exploited by various stakeholders through different means and without their consent [1].

The HIPAA validation method is used in this model in order to apply the security rules, the information is stored in the software and is used to communicate with the devices. OmniPHR[17] model was introduced in order to deal with some issues regarding security and data privacy. Because of PHR contexts, there were some issues in the OmniPHR model. This issue is related to the data replication and multiple providers accessing the data and the data syncing. Another method called the EHR model proposed an idea for data sharing and monitoring in the health organization. P2P method was implemented. The Electronic health record model was to replicate the data in a different health organization when there was an update in the patient’s record.

Ethereum is a public blockchain platform [18], with the possibility to create smart contracts and focuses on Blockchain technology development. A Smart Contract is a computer-based protocol, consisting of rules, agreed by the stakeholders according to their requirements and also it has a Turing complete architecture for securing the patient’s data and the rules that can also be modified by the legal person whose signature is in the agreement [19]. A Smart Contract is also used to interact with the blockchain and healthcare providers according to their need, and also manages the access to the patients healthcare records given to the stakeholder and secured administration [20].

VIII. Results and Analysis

Over the decades, there have been a number of research going on in the field of Healthcare to detect the fraud. There are a lot of complications in the way medical data is stored or related to other systems. Rashidian et. al [21] has outlined the fraud detection using the data mining methodology. Tahir et. al [22] suggested a statistical methods in the assessment of the fraud using data mining approach. Bauder et. al [23] presented the machine learning approach using LEIE database and mapping of fraud labels.

All these researches have been leveraged by the Machine learning or the data analysis technology by the addition of extra security module to provide data privacy. In our paper we use HIPAA validations in order to process the data for EDI claims and provide the feature of sharing the insurance claims among the interested parties by leveraging the blockchain technology. There are many rules posed by government like HIPAA, to regulate the sharing of information. Each hospital, insurance companies, medical practitioner maintains their own local set of copies making it difficult for patients and their dependents to access their information. However, having medical records stored over distributed ledger like blockchain, it would form a single origin of authenticity for the stored as well as their related records. Since the records are spread over multiple system (ledgers) the access can be granted to additional parties like hospitals, doctors and insurance companies.

This architecture would drastically increase the understanding and collaboration between multiple parties, reducing the overhead of sharing data over different protocols and providing great accessibility to data. Now multiple Insurance companies can track the patient activity by accessing the blockchain network. When a patient claims for a certain amount from an insurance company, the company checks for particular information like reason for visit, claim amount, and other Identifications of patient. Using this information, the company can generate a transaction with the network. After the transaction has been approved, a logical block is created in the network that represents this transaction. This transaction is viewed by everyone participating in the network. The next time when the same patient visits another company to claim, the company can now check for the patient details across blockchain. If claim matches with the previously committed transaction on the network, the request for the claim will be denied to the patient. This methodology can also be used to avoid doctor shopping.

The decentralization of medical records enhance the security of stored data. Moreover, peer-to-peer sharing of blockchain makes it impossible to make modification to a block of storage without modifying the whole blockchain network. Patients can also have the ability to define how and with whom their records can be shared. Providing "who can access what" information in blockchain is not straight forward. Since, the information is accessible by everyone participating in the party, there should pre-establishment of additional protocols and design to add additional security. To accomplish the entire flow, a log was maintained to record the connectivity between multiple services, the API exposed. Gathering necessary information and related articles was prolonged due to lack of actual implementation and documentation of health care on blockchain.

In this work we have faced problems related to selection of databases for HIPPA validation and set up of blockchain network to create the distributed network. At current software industry, only two open software are highly used such as BigchainDB and Ethereum to create the distributed network. Ethereum is well known blockchain technology in the market but it offers private blockchain features so that only one node in the network (controller) will be having the write permission to create transactions and others node in the network be having only read permission. This technology will be mostly used to create crypto currency wallet applications.

To create the network with all the trusted nodes with create asset permission, which is essential features we wanted since each node in the blockchain network represent insurance companies and each insurance companies should have the permission to create and access transactions, we have to use the BigchainDB technology which provides the public blockchain features to give every node in the network with write and transfer permission. The problem with the BigchainDB is that we do not have the stable version of it and community support, and its specific version of release works only with specific version of Tendermint and RPC. we had to try with the different version of BigchainDB and checks its dependencies with the other dependent software.

perform validations related to claim, we wanted a graph flavor database such as Noe4j but BigchainDB supports only MongoDB to store the assets as it needs to provide the consistency and availability of the data across all the nodes in the blockchain network. So, to perform the validations of the user insurance claim we used Neo4j database and after its transaction we stored the asset in the MongoDB database of BigchainDB network to make the asset available across all nodes in the network.

IX. Conclusion

Although evolving blockchain technology is expected to affect technological advancements in future, its capabilities seem especially appropriate for the pharmaceutical and healthcare industries and their complex data-sharing requirements. The findings and results shows that, the use of blockchain in storing health information can be effectively secured by having data over multiple machines which are supervised and authorized by distributed community in preference to centralized approach. This method provides a way for everyone in the party to view and verify data that is added and modified. Moreover, there is a record of each and transactions and modifications done within the network. The performance of middleware to parse and transform medical health data is fast and there is not much observable delay to load that processed data into blockchain.

References

[1] Tawalbeh, Lo'ai A., and Hala Tawalbeh. "Lightweight crypto and security." Security and Privacy in Cyber□Physical Systems: Foundations, Principles and Applications (2017): 243-261.

[2] S. K. Simon, K. S. M. Anbananthen and L. Seldon, "A ubiquitous personal health record (uPHR) framework," 2013 international conference on advanced computer science and electronics information",vol. 41, pp. 423–427, 2013.

[3] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", 2016 2nd International Conference on Open and Big Data (OBD), pp. 25-30, 2016

[4] S. Wang , J. Wang, X. Wang, T. Qiu, Y. Yuan , L. Ouyang, Y. Guo, and F.-Y. Wang, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach", IEEE Transaction on computational social system, vol.5, no.4, December 2018.

[5] R. Kelley, "Where can $700 billion in waste be cut annually from the US healthcare system," Ann Arbor, MI: Thomson Reuters, vol. 24, 2009.

[6] H. Huang and Z. Dong, "Research on architecture and query performance based on distributed graph database Neo4j," 2013 3rd International Conference on Consumer Electronics, Communications and Networks, 2014.

[7] "Financial Crimes Report to the Public," FBI Report, 2007.

[8] National Health Care Anti-Fraud Association (NHCAA), "Guidelines to HealthCare Fraud: Factsheet," 2002.

[9] Lo'ai, A. Tawalbeh, and Suhaila Habeeb. "An integrated cloud based healthcare system." In 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, pp. 268-273. IEEE, 2018.

[10] E. A. Duman and S. Sagiroglu, "Health care fraud detection methods and new approaches," 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, 2017, pp. 839-844. doi: 10.1109/UBMK.2017.8093544.

[11] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise Components Processes and Problems", IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, 2018.

[12] Gokai Saldamli and L. A. Tawalbeh. "When Healthcare Services Meet Blockchain Technology", Book Chapter in: Maleh, Y. (Ed.), Shojafar, M. (Ed.), Alazab, M. (Ed.), Romdhani, I. (Ed.). (2020). Blockchain for Cybersecurity and Privacy. Boca Raton: CRC Press, https://doi.org/10.1201/9780429324932.

[13] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla and K. Shuaib, "Introducing blockchains for healthcare", 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

[14] G. Yang and C. Li, "A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems," 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, 2018, pp. 261-265. doi: 10.1109/Cloud-Com2018.2018.00058.

[15] Tawalbeh, Mais, Muhannad Quwaider, and A. Tawalbeh Lo'ai. "Authorization Model for IoT Healthcare Systems: Case Study." In 2020 11th International Conference on Information and Communication Systems (ICICS), pp. 337-342. IEEE, 2020.

[16] Bhatt, Smriti, A. Tawalbeh Lo'ai, Pankaj Chhetri, and Paras Bhatt. "Authorizations in cloud-based internet of things: current trends and use cases." In 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), pp. 241-246. IEEE, 2019.

[17] S. Safavi and Z. Shukur. "Conceptual privacy framework for health information on wearable device". PLoS One 2014; 9:12.

[18] A. Roehrs, C. A. da Costa and R. da Rosa Righi. “OmniPHR: a distributed architecture model to integrate personal health records”. J Biomed Inform 2017; 71: 70–81.

[19] G. Wood, ”Ethereum: A secure decentralised generalised transaction ledger”, Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[20] M. Wohrer and U. Zdun, ”Smart contracts: security patterns in the ethereum ecosystem and solidity”, Blockchain Oriented Software Engineering (IWBOSE) 2018 International Workshop on, pp. 2-8, 2018.

[21] P. Zhang, J. White, D. C. Schmidt and G. Lenz, “Applying software patterns to address interoperability in blockchain-based healthcare apps”, 2017. [Online]. Available: https://arxiv.org/pdf/1706.03700.pdf

[22] H. Joudaki, A. Rashidian, B. Minaei-Bidgoli, M. Mahmoodi, B. Geraili, M. Nasiri, and M. Arab. “Using data mining to detect health care fraud and abuse: a review of literature”, Global Journal of Health Science, 7(1):194–202, 2014.

[23] T. Ekin, F. Ieva, F. Ruggeri and R. Soyer. “Statistical Medical Fraud Assessment:Exposition to an Emerging Field”, International Statistical Institute, 86(3): 379-402, 2018.

[24] R. A. Bauder, and T. M. Khoshgoftaar. “The Detection of Medicare Fraud Using Machine Learning Methods with Excluded Provider Label”, The Thirty-First International Florida Artificial Intelligence Research Society Conference (FLAIRS-31), pp. 404-409, 2016.