Grenze International Journal of Engineering and Technology, Jan Issue

Tamperproof Health Information Exchange System using Cyber-Security

Praveen S[1] and Dr. S.Kuzhalvaimozhi[2]
[1-2]The National Institute of Engineering, Department of Information Science and Engineering, Mysore, India
Email: praveenrohit98@gmail.com,ishod@nie.ac.in

***Abstract*—In the present world, the uses and need for Health Information Exchange (HIE) are vast. Providing best-effort delivery of patient treatment is also necessary for saving lives of mankind with faster Coordination and determined Commitment are the most needed criteria, every hospital must adapt to a greater good. The National Coordinator for Health Information Technology (ONC) is finding patient-centered HIE systems which can give managerial control over the data. In the present world, the health systems are facing several challenges to secure the information of the patient and provide them at the right time because of the fact that if any delay may cause life harm to the patient. there are a lot of issues in providing security and privacy to the data. To withstand all these issues the Blockchain is a unique solution in the current technological standards. Blockchain is viewed as an "unhackable" form of the security providers, it can deliver the best form of solutions to these types of problems. We have developed a blockchain model to provide security to the data and privacy to the treatment reports of the patient together this ensures data Provenance and gives access to complete records of the patient to their control. The accomplishment of this solution will fetch patient-centric HIE by personalizing data segmentation and creating an "authorized list" for doctors to access their data. This patient-centered HIE process evaluated the model's feasibility, stability, security, and robustness quantitatively.**

***Index Terms*— Blockchain, Health Information Exchange(HIE), Electronic Health Record(EHR**

I. INTRODUCTION

In Health Sector, to maintain Health records some systems are widely utilized around the world, One of them which is most popular is the Electronic health record (EHR) where this system is accompanied by non-federal acute care hospitals in the United States adopting a rate of more than 96 percent[4]. There have been incentives given by the associations under the act of Economic and Clinical Health (HITECH) which was abolished in the year 2009[8,9]. The usage of HIE is also encouraged by financial incentives created by the Health Information technology for Economic and Clinical Health Act in the year 2009[6,8,9]. This System across healthcare is shown to be highly beneficial in terms of decreasing Health care expenditures and increasing quality of care and providing enormous disease or problem observation. The organizations like National Coordinator for Health Information Technology have spent and funded a huge amount of financial supplies to bring up the name and

Grenze ID: 01.GIJET.9.1.610

meaningful uses of HIE(Health Information Exchange) networks and the creation of health information exchange (HIE) networks. Above this investment, there has been a noticeable amount of progress in this field improving business firms in the same collaborative association, such as state-wide hospital systems. HIE usually reduces emergency department usage and cost in some cases if used properly and implemented in the trusted health platforms [7]. Above these methods there have been surveys taken up by the AHSP national Survey of pharmacy practice in the hospital trying to set their focus on enhancing and managing the medication -use system and the pharmacist also has the role of achieving this enhancement [11].There are many numbers of HIE systems providing issues in terms of data quality which can bring the poor presentation of data representation, data security which is having a risk of a sensitive data breach, patient privacy leading to leakage of information, and patient participation not much accepted from the patients. Furthermore, there have been recent indications of a move to interoperability that focuses on the patient although consumer-mediated exchange. There are 3 existing HIE forms. They allow patients to manage their health information online and get in touch whenever needed. To establish a true patient-centric HIE, patients must have a full hand in control over their data, including permitting a healthcare facility's data access, decidingtheir information which can be sharable and non-sharable, acknowledging the use of data, and accepting the shared data's life cycle. Security and privacy concerns, data thefts caused by illegal ingress to the patient's health records, and data discrepancy between the obscure provider's electronic health records data and the receiver's data are all issues that existing health information exchange systems face. Finally, there are securityissues with data interchange that can be addressed utilizing the blockchain approach. A systematic review andexamples in Health care have collected details regarding underlying Blockchain platforms[5]. A Blockchain is a transaction ledger in a distributed fashion which is composed of blocks with each block indicating a set of transactions[2]. Blockchain is a network that is distributed and peer-to-peer communication-enabled technology, that conducts transactions without the involvement of a third party and an open-source platform that allows all users to make transactions without mediating party[1], the transaction will be broadcasted to allusers, including patients and clinicians, by auditing and checking whether the sender's access key matches therecipient's access key. Health companies and organizations have been collecting data to personalize services and improve the decision-making process in the health sector[12]. Blockchain requires huge computational power and more oh input and output operations, making it impossible to run a blockchain node on mobile devices (IoT devices) which usually have less memory and less power in computation[14]. Electronic Health records are having highly variable levels in data accuracy measures that can be ranging from 30% to 100% data exactness and completeness[10]. A blockchain under permission will avoid the replications of transactionsof the service at the endpoint on the set of blocks of entities with a service having a common interest[13]. Blockchain is having great potential in achieving the future of internet systems[15]

II. Rationale Using Blockchain Model For Patient-Centric Hie Applications

There are different conceptual models of different HIE systems:
Three forms of health information exchange :

1. Directed Exchange: Directed Exchange is a type of health information exchange method used by a health care provider to securely transfer the details and information of the patient to another health care provider, care coordinator, or other Health Information exchange Organization
2. Query-based Exchange: This is an exchange where there is an ability or provision for providers to search find or request details or information on a patient from other Health care providers.
3. Consumer mediated exchange: The consumer mediated exchange is a method that allows the patientsto get hold of their health care information online just the way they control or manage their finance and banking work online.

Blockchain Solutions for Patient-centric HIE challenges:
One of the main obstacles in accomplishing blockchain technology to manage patient data is the fact if that data is already being managed by present systems. Time and money have been used a lot in building these architectures and introducing new technology would require rebuilding part of the platforms.
In the present systems, patient information is stockpiled in local databases with some of the few possibilities of sharing it between multiple organizations and hospitals. Blockchain technology would make an impact that can bring complete change which is moving from technologies that are small scale and centralized to worldwide systems that will be distributed in nature. However, it is proof that it would bring a collaborative and

interoperable work environment between the medical field and scientific communities which can allow innovation to grow in this technical world. While some still think that this is not worth time and money
In this present-day healthcare organizations are spending heavily on electronic medical records. This is a nice initiative step in creating a digital platform for uniting all types of patient health information in one place whichcan be readily available during emergencies and during any type of time-sensitive situation. We can also achieve move the data to the cloud platform and can implement Blockchain technology which can provide security and privacy to data finally managing the access and authorization part will be finalized. Analyzing Blockchain technology from a technical perspective, some of the medical records will include files that are large in size, those files would probably be stored in off-chain databases and some particular cloud computingsystems which can manage bulk data, and only hash would be kept in track to the blockchain. So, for such conditions, the electronic papers must be stored in the first place and papers having less need are being abandoned. Hence, for blockchain technology to co-exist with architectures, there is still a long way and several things that need to be accomplished

III. METHODOLOGY

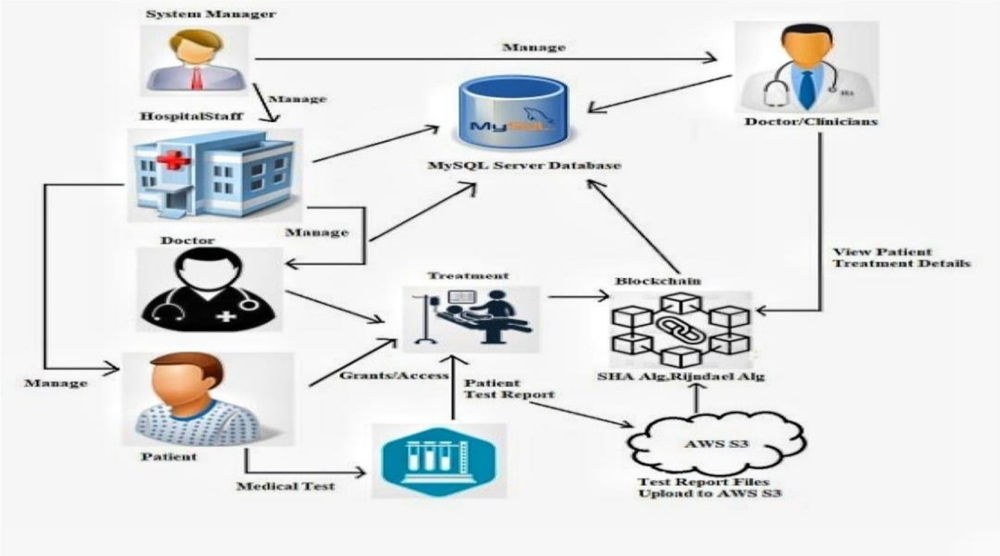

Figure 1. System Architecture of patient-centric HIE

To make use of the different and unique technical potential of blockchain for patient-centric HIE, Here we have accomplished an efficient and secured platform for communication.
The blockchain can be implemented using the Ethereum platform but here we have implemented the same functionality that Ethereum is performing, in the SQL database platform. The application creates touchpoints between two entities who need service from each other.
If the patient is new to this website, He has to create an account where a unique ID will be generated and he has to maintain separate Login credentials for his account to check his details for his use. Upon visiting a hospital, the patient has to submit this Unique ID to the Hospital which is using this web Application and he can take the treatment from them. The hospital will Document all the basic necessary details of the patient for future use during his consultation. All the treatment details will be stored in a database and it will be uploaded from the hospital in the backend, this data will be encrypted using the SHA Algorithm, AES Rijndael Algorithm, and Blockchain and will be stored in the database. This data will be secured in the database and isused in the future. When the same patient visits another hospital over some time and consults another doctor for his disease the doctor will examine his previous reports now this part is done through the application we have developed. The hospital Uses the same Unique ID provided by the patient and the doctor will request forthe system manager of the Application to view his previous treatment records by raising a

view request. Now the request will log into the system manager which needs to be processed and replied to. After checking the valid credentials of the doctor who is raising a view request to the system manager, if the Authentication is verified the system Manager will send the data to the doctor. Here the data that is Encrypted will now be decrypted using the same Algorithm and will be displayed to the doctor with a tampered Attack Status visible in either Green or Red Colour if the status is green the message is safe and it is free from tampering. If the status is red the message will not be displayed and the doctor has to raise another request to the system manager to send the tamper-free Information again. Now the system manager will be having the support of blockchain technology to store this information and the same copy of Information will be present in Database 2 and Database 3, which is free from Tampering and secured to resend the correct information to the doctor with the Tampered Attack status visible with green colour. The doctor can even get information about differenttreatments which were given to different patients by searching in the search tab of the Application using the keywords support. These keywords are specific to particular treatments and the doctors can access them for their future references.

IV. IMPLEMENTATION :

To establish a secured communication medium between the patient and the hospital management people, a separate identification code is given to each personnel, its credentials will be in the form of a user ID and password. If an authorized user from the hospital side wants to get a request solved from the application, He has to provide the right login credentials and can enter into the application for further uploading of the details or fetching of information that he desires.

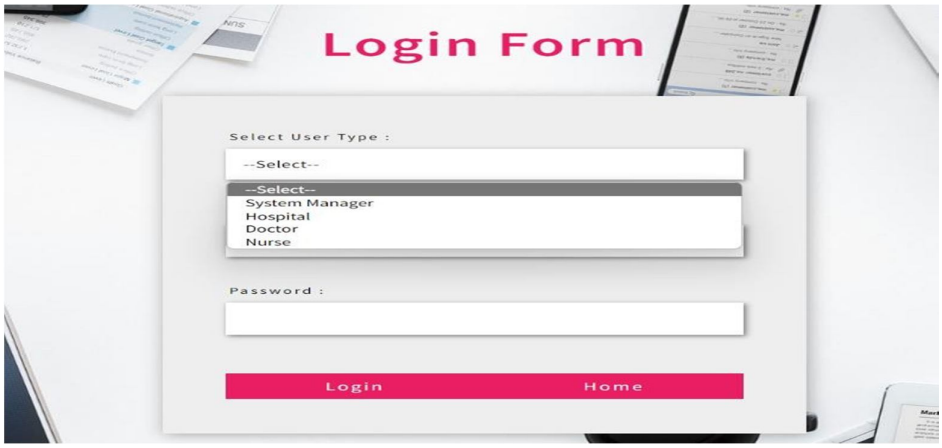

Figure 2. Login form of the Application.

System manager: The system manager will be maintaining all details of the hospital, doctor, patient, and nurseand will be having the access to add hospital and under which department the patient needs to be treated. Also,can add the medical test and its details if necessary.
Hospital: When a hospital is being added by the system manager now hospital will be having the access to addthe doctor, nurse, and patient details for future use and the previous health records of the patient can also be stored for verification and understanding of the problems of the patient during his treatment.
Doctor: The doctor can add treatment of the patient according to the dates and basic information about the treatment which the patient has taken. For this step the doctor has to first Login to the application with the login credentials, the has to manage a patient with the patient details like name and ID and then will have the accessto enter the treatment details and disease information which the doctor has diagnosed
Nurse: The nurse can view the medicine prescription details entered by the doctor to cure the patient and can follow up with the same procedure if the patient is needed under the advice of the doctor.
The System manager will operate all the functions and task that needs to be executed by assigning each task to authorized personnel. The data will be maintained by a server maintenance team who is responsible to resolvethe requests that reach the server from the hospital side. For example, there is a request from the hospital to viewsensitive

information this is resolved by decrypting the information and sending it to the respective team in thehospital who had raised the request.

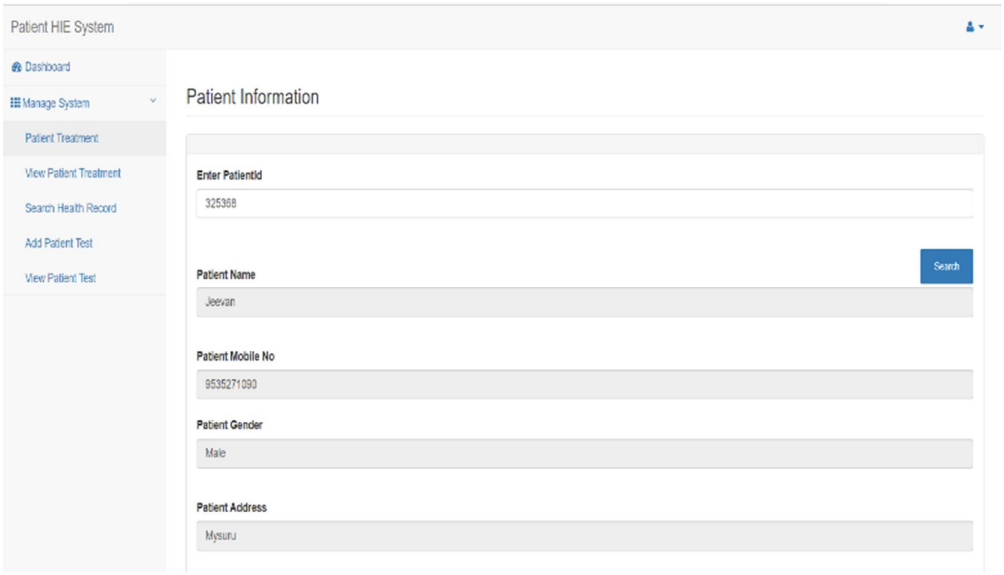

Figure 3. Patient information fetching using User Id

As provided with the unique Id of the patient, based on that Id doctor will fetch the primary and basic info ofthe patient whom he is treating. In Fig 3 we can observe the patient details are being displayed after providingID and search instructions. The services that a doctor can get are also visible in Fig 3. A doctor can performadding records of the patient and get the information of the previous treatment history and details if he is facingany issues in providing medications to other patients

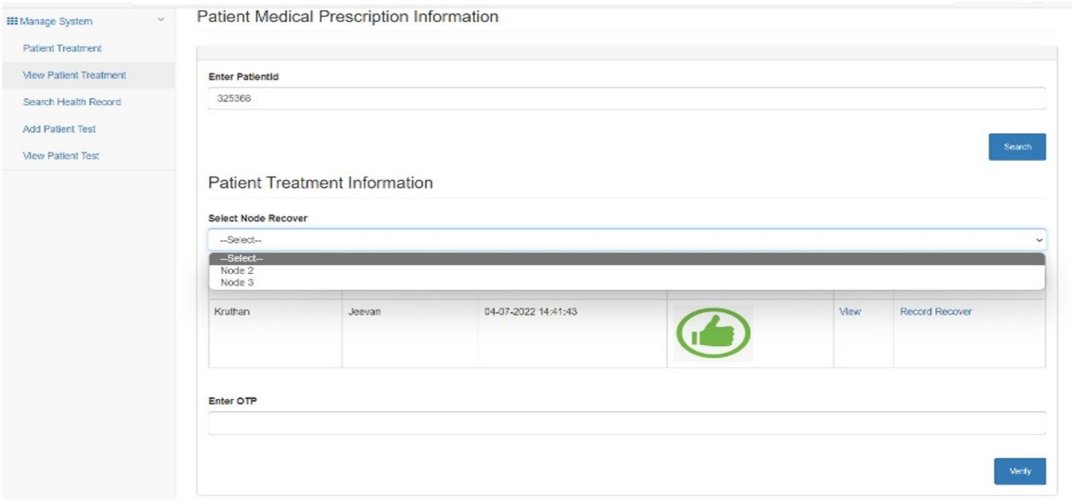

Figure 4. Doctor viewing safe Report

A doctor can view the report of the patient during treatment. Fig 4. Shows the name of the patient, doctor, andthe log date the status shown in the figure conveys that the report is safe to view and there are no signatures of tampering. He can view records by just providing view instructions in the application. There is an OTP(One-time password) validation step for viewing the Health record.

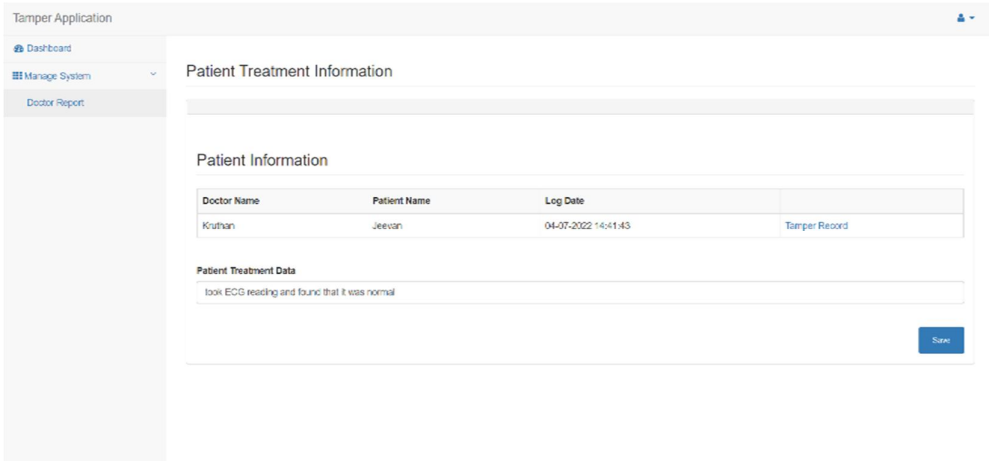

Figure 5.Tamper Application

Here the hacker can tamper with the record of the patient. Once tamper record instruction is given, the patient treatment details are visible and he is having the access to change the data and save the wrong data in the database where it was fetched. This application is developed because any sign of cyber attack may lead to data loss and privacy issues to be ready with the situation this tamper application is developed for better understanding

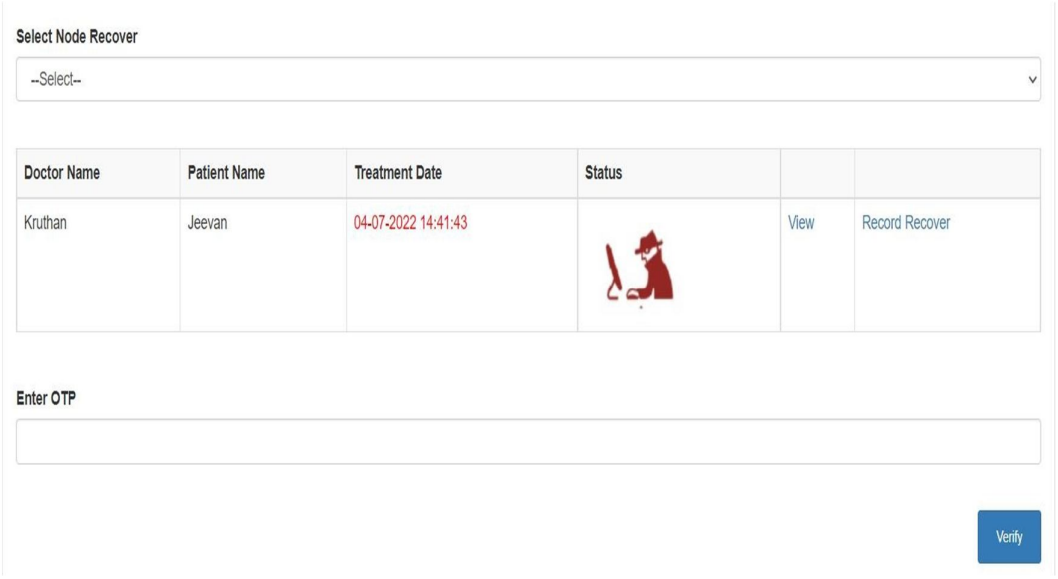

Figure 6. Record status in the application after tampering

Supposing, the doctor needs a record and he requests it, the status of the record will be shown like in the above Fig 6. View option will be disabled. First, the record has to be recovered by selecting the node from where the data needs to be recovered. After recovery, the data will be ready to view

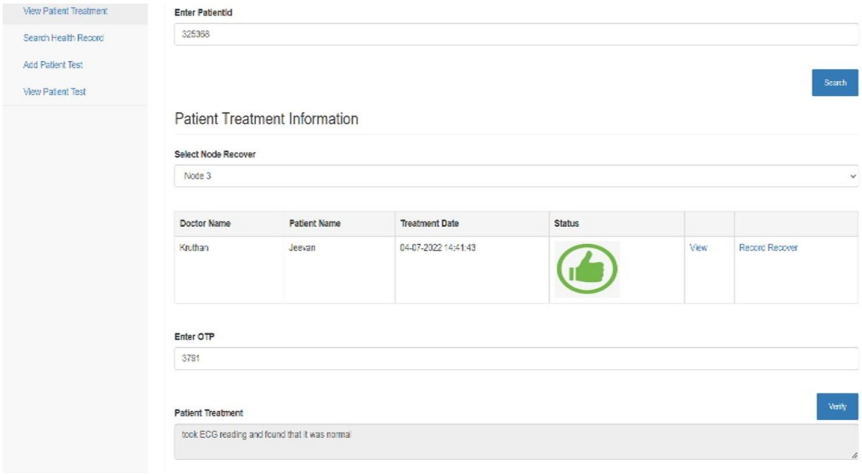

Figure 7. Status of the report after Record Recovery

After recovery, the status of the report will be like as shown in above Fig 7. The view will be enabled after anOTP validation the record information will be visible to the person who ever is accessing it.

*SIMULATION:*The doctor will log in using a user ID and password and will manage the patient's treatment. At first patient, ID is entered and a search input is given, to get the basic and primary information about the patient before analysis. When the search input is given in the application, based on the ID programmed in the backend will fetch the primary details like gender, mobile number, and address information. This searching and fetching aredone under SQL adapter in the database.

The doctor provides the treatment information of the patient and a search keyword of that treatment. This search keyword is to get the details whenever necessary in a shorter time. For example, if the treatment is givenbe an angioplasty for a patient who is having heart-related disease the keyword can be 'Heart Problem'. If thiskeyword is entered in the search tab all the treatment details and procedures will be displayed. All this information will be stored in databases.

Backend: When the save instruction is given, based on the doctor Id it will convert the patient treatment into a byte in other words it will get converted into data that can be stored in tables in SQL. These tables are created dynamically whenever the data is being entered and saved.

*Data Encryption:*For the encryption of the treatment details the AES Rijndael algorithm is being used, For the digital signature and hash code generation SHA algorithm is being used, and storing these sensitive data in blockchain- implemented platforms with the help of AWS S3 services to allot the path for the data in the database.

Hash code Generation: SHA Algorithm is used to generate hash code for the given data. When the first entry is given, the previous hash value would be taken as 0. Doctor Id, Patient Id, search key, and log date are detailsthat will be given as Input to the SHA Algorithm to generate hash code for that data. For the next entry, the hash value that was generated for the first entry of data becomes the previous hash value to this entry and the hash code is being generated. The hash code length would be of 32-bit length.

Data Encryption: AES Rijndael is the algorithm used for encrypting patient data. The first two characters of the hash value will be converted into ASCII, this value along with patient treatment will be encrypted under AES Rijndael Algorithm. This is rigged up programmatically using a namespace called '.cryptography' and a built-in class called Rijndael manager is being used. Necessary elements required for secured encryption of data will be provided programmatically in the application. After encryption, this data will be stored in the table which was created dynamically for the first entry of the patient's treatment. This is an unbreakable block cipher because the number of transformations the data will be processed will be 10 rounds, which makes it more powerful compared to other algorithms. Hence AES Rijndael is the most secure algorithm for data encryption.

Tampering: Here a separate application is used to create tampering of data to achieve a system that can withstand both attack and repair from the authorized person's perspective and hacker's perspective. Both are kept in the notice and a full system of communication comprises both possibilities that can take place during sensitive information exchange. Thus, helping us to understand better from both perspectives. The data is first obtained using API calls in the network. The data will be viewed by the hacker and can change the correct report with his incorrect values. This false information will be saved in the database. Along with this, the hacker will use his log date and sequence number to generate a new hash value and replace the correct hash value with his newly generated hash value which makes it impossible for the decryption side to decrypt the encrypted data appended with this new hash value.

Data Retrieval: The tables that were generated dynamically when the entries were given will be having the data which is encrypted. If any chances of tampering with the same set of data with original hash value and encrypted data will be stored in another two databases. These databases can be called nodes. When the information is about to be viewed it will show the status of the data whether it tampers form or original form. If it is free from attacks, it will give a view access to the doctor to see the record. If tampered it will show a tampered notification of that data being hacked or changed. Now the user will be given access to select the node(database)from which he wants to recover the non-Tampered data. View access will be disabled if the data is being tampered. After selecting the node for information recovery an OTP Verification has to be made to view the data from the other two nodes.

V. Results And Discussion:

We have simulated the data requests from the healthcare organization side by developing an application that is efficient enough to process the request and provide best-effort communication.

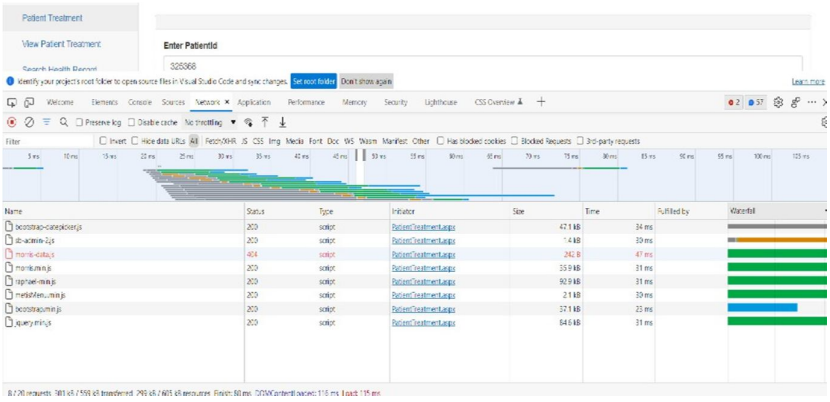

Figure 8. Behaviour of the Application

The transactions are able to process the request from the 20ms to 5000ms range. The speed of the network to process and respond to the request will be ranging within this particular limit of time scale. The new set of entries will be tabulated in new tables because the Id differs from one another. If the same patient is having multiple types of data to be stored, a table with the respective patient Id will be used to store the data. Hence, we have developed an efficient and secure medium for electronic health record transactions. This application will give the best-effort delivery of service to healthcare organizations in maintaining health records and in making them available at the right time

VI. Limitations :

The limitations of the application are

1. Risk of server failures
2. Delay in network
3. Resources unavailability may lead to incomplete information
4. Node maintenance must be kept up to date for proper recovery of data

Many times there is a risk of servers getting failed to provide data some of the reasons are overheating, hardware issues, software issues, cyber-attacks, and system overload these may cause server failure when the request arrives. The network can also be the reason, which can reduce the efficiency of the application by reducing the speed of fetching the data. If the strength of the Channel is weak it may result in an excess delayin processing the request. Not providing proper resources to the application may lead to incomplete information, which can harm the service by misguiding. Node maintenance is most needed to handle the data during critical times. if they are not maintained there can be possibilities if information getting lost or junk value can get occupied.

VII. Future Work :

The application stores all the log files but an enhancement can be made like the patients can check the details of who has accessed their data. staff can have access to check the EHR (Electronic health record) data, which can ensure data provenance. All the authorized persons must be made to check the data only from the trusted health care facilities. For upcoming enhancements, we can make use of artificial intelligence components andapply that to blockchain which can allow researchers to retroactively study HIE outcomes. Decide which cannot be established in the existing HIE systems. Our upcoming work can continue to evaluate the blockchain protocol to fundamentally resolve the scalability issues by re-engineering the time and resource-consuming mining processes of the blockchain system under privacy.
Resilient business prototypes can be made using blockchain. Nodes can include a credit mechanism to give users a separate incentive to join the system. The health care facilities can also receive incentives for providingdata or any type of service to other facilities, patients can also receive credits for giving their data to researchers,which can help their research project. credits can also be used to acquire data in return.

VIII. Discussions And Conclusions:

The distinctive contributions of this work incorporate giving the following practical components to the blockchain system to achieve patient-centric HIE: (1) nodes set up to communicate with users which may include sending and receiving health records and provide a convenient graphical user interface for the users to have a good visualization and interaction with the application during usage. (2) Best use of algorithms is being made which provide assurance to data security and privacy. (3) if there is a large-scale implementation of this application is done there will be feasibility, stability, and robustness in the service provided by this blockchain model for the HIE applications.
It is noticeable to mention that blockchain technology is not only the solution for HIE. This paper illustratesthe feasibility and robustness of using the unique features of blockchain technology in HIE for the Health community to consider applying the variations of the blockchain technology for HIE tasks, as well as to evaluate regulations and policies to adopt this emerging technology.

References

[1] Blockchain Distributed Ledger Technologies for biomedical and Health care Applications ,Tsung-Ting Kuo,Hyeon-Eui Kim and Lucilaohno-Mchado,2017
[2] A Blockchain based approach to Health Information Exchange Networks, Kevin Peterson,Rammohan Deeduvanu,Pradip Kanjamala and Kelly Boles Mayo clinic,2020
[3] Applying Blockchain Technology for Health Information Exchange and persistent Monitoring for Clinical trials ,yan Zhung ,BS,Lincon Sheets ,Zoyin Shae , Jeffery J.P, Chi Ren-Shyu ,2021
[4] A Pateint centric health Information Exchange Framework using Block chain Technology ,Yan Zuhang lincon R sheets ,Yin-wu chen , Zon yin shae , Jeffery J.P , Chi Ren shyu ,2020
[5] Comparison of Blockchain Platforms: asystematic review and health care examples ,journal of American Medical Association ,tsung -Ting Kuo , Hugo Zavaleta Rojas ,LucilaOhno Machado ,2019 .
[6] Usage and Effect of Health Information Exchange , Robert S.Rudin,Aneesa Motala Caroloine L , goldzweigand Paul G Shekelle.
[7] R. S. Rudin, A. Motala, C. L. Goldzweig, and P. G. Shekelle, "Usage and effect of health information exchange: a systematic review," Annals of internal medicine, vol. 161, no. 11, pp. 803-811, 2014.
[8] Health Affairs ,Saurabh Rahukar ,Joshua R , Vest and Nir Menachemi,2015.
[9] Choosing wisely clinical and decision support and adherence and associated inpatient . The American jounal of managed care ,August -2018