BlocHIE: A Blockchain-based platform for Healthcare Information Exchange

Sanjay N[1], Yashwanth A N[2]
[1,2] Atria Institute Of Technologoy

Abstract- *With a great number of development in the field .of Internet Of Things a huge amount of data is generated at each and every second from both the hospitals and individuals.To store and share such a large amount of data is a challenging task. In this paper we propose BlocHIE which is a blockchain based platform for Health Information exchange. First we analyse the different requirements for storing and sharing such a large amount of data. Based on the requirements we make use of two loosely-coupled Blockchain to handle different kinds of data. Second we combine the off-chain storage and on-chain verification to ensure the safe transfer of data. Third we use two transaction packing algorithm to improve the system throughput and maintain the fairness among the users.*

Keywords- Cloud computing, Internet Of Things(IOT), Blockchain, Cloud service providers, Distributed Ledger, Consensus, Proof of work, Cryptography, EMR & PHD chain, Throughput-first, Fairness-first

I. INTRODUCTION

The sharing of HIE among the hospitals has several uses such as they can enhance the understanding of each clinical records and the reseraches can get a better view over the test results.The huge amount of data generated by the IOT devices was handled by the cloud computing in the early stage.But the cloud service providers failed to provide the services to store and share such large amount of data.One more risk factor was that there is a chance of data being exposed to malicious users.Fortunately a new technology replaced the cloud computing which is known as Blockchian which has the attractive features such as security,privacy.

There were two main problems with the Blockchian the first is they were only storing the electronic medical records ignoring the personal healthcare data.The second problem is it stores the electronic medical record in an complicated access environment.To solve the issues which is mentioned above we propose a BlocHIE-a Blockchain based platform for healthcare information exchange.In this we propose two lossely-coupled blockchain such as EMR-chain and PHD-chain to maintain the security and accessability.For both of these chain we propose transaction packing algorithm to improve the system throughput and maintain the fairness among the users.

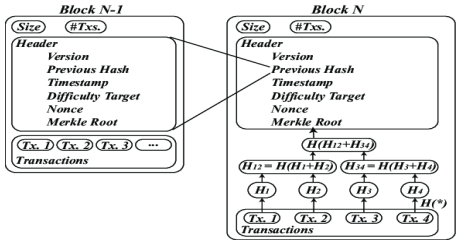


Fig 1:structure of Blockchian

The below diagram shows the structure of a traditional blockchian which has four components namely block size,transaction counter,header and transactions.The header has six fields namely version which represent the version number,timestamp which tells the approximate time for creating the block,merkle root which has the hash value of all the blocks,previous hash which has the hash value of previous block.

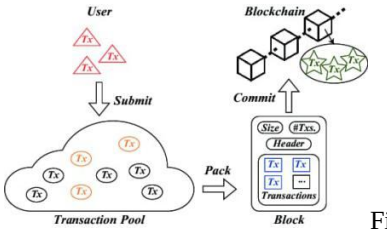


Fig 2:procedure for commiting transaction

There are three steps involved in commiting a transaction at first the user submits the raw data which will be sent to each and every member of the transaction and each will recieve a copy of the raw transaction and the consensus as two steps one is packing and one more is commiting.At packing each members select some transaction and put them into a block which are called as uncommited blocks and incase of commiting the uncommited blocks are validated and verified and the uncommited blocks are commited.

II. SOFTWARE DESIGN AND IMPLEMENTATION

There are mainly three components in an BlocHIE one is blockchain network,second is hospitals and the third is the individual who are willing to share the data.

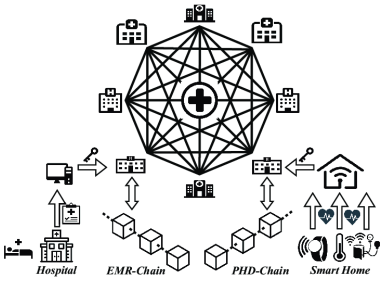
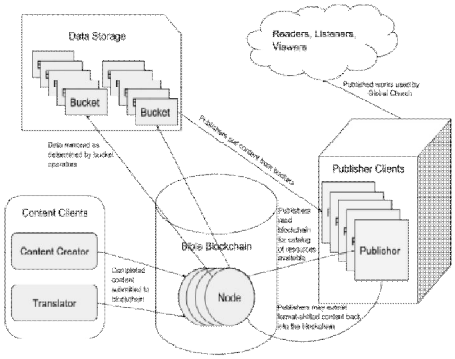


Fig 3:BlocHIE system architecture

Among the three components there are two parties who are submiting and sharing the data.For the hospitals for sharing the data are highly sensitive.But when it comes to the data genearted by the individuals the concern is about the quantity.We use two loosely-coupled blockchain such as EMR-chain and PHD-chain for transfering the data to the blockchain network.If both the patient and the hospital agree to share the data then the data will be shared through the EMR-chian with both the hospital and owner signature.The data generated at the smart homes are shared with the PHD-chain with only the owner signature.

B.Off-chain storage and on-chain verification

Fig 3:Emr chain



When a medical record of a patient is generated at the hospitals three copies of the data will be generated.The first copy will be stored in the hospital database and the second copy is sent to the patient.The third copy will be different from the two copies and it has the timestamp,hospital signature,owner signature,previous hash and keywords.

The advantage of such structure is they are not publicaly accessible.It reduces the system throughput and accessability is preserved.Off-chain storage is achieved by storing in the hospital database and on-chain storage is achieved by including the previous hash of the medical record.

C.Transaction packing algorithm

When the blockchain network wants to get some transaction commited each node is supposed to follow the procedure that the nodes are supposed to select the some transaction from the pool .Different transaction can have a different waiting time .It can increase the the throughput to pack as many transaction as possibleIt can enhance the fairness to pack those transactions.FAIR-FIRST and TP&FAIR, to coordinate the nodes in the Blockchain network. The algorithms are shown in Alg. 2. FAIR-FIRST is used when fairness is critical in the system while TP&FAIR sacrifices a little fairness for higher throughput. The two packing al-gorithms can be selected based on the required features of the Blockchain-based system. In our system, PHD-Chain is designed to use TP&FAIR for high throughput and moderate fairness while EMR-Chain is designed to use FAIR-FIRST since throughput is relatively less important. The intuition for the FAIR-FIRST packing algorithm is to let all the nodes work on the same transaction combination, which is of the maximum fairness. The intuition for the TP&FAIR packing algorithm is to let the nodes work on different transaction combinations, while can achieve top fairness respectively.

Throughput-first and fairness-first packing algorithm

```
procedure TP&Fair(X)
  m ← the maximum number of transactions
  in a block
  X'←App-Kth-Sum(X,|X|,m,i)
  return X'
end procedure

procedure Fair-First(X)
  m ← the maximum number of transactions
  in a block
  X'←App-Kth-Sum(X,|X|,m,1)
  return X'
end procedure
```

Similarly, we can get the corollary that the larger the sum of the waiting times of the transactions is, the larger the fairness is. To this end, we can get the strategies to pack transactions with the largest, the 2-nd largest fairness and etc..Actually, we do not need to solve the KTH-SUM problem exactly. Instead, we only need to find an approximate solution. Hence, we propose the algorithm APP-KTH-SUM as shown in Alg. 1. separate the subsets level by level. For a subset in a lower level, there must be a subset which has larger subset sum in the upper level. The level is determined by the sum of the index.

III.TESTING AND ANALYSIS

To demonstarte the effectiveness of a BlocHIE we are going to implement a BlocHIE in a minimal viable product.The below figure shows the implementation of a BlocHIE which has three layers namely communication layer,Blockchain layer and GUI layer.

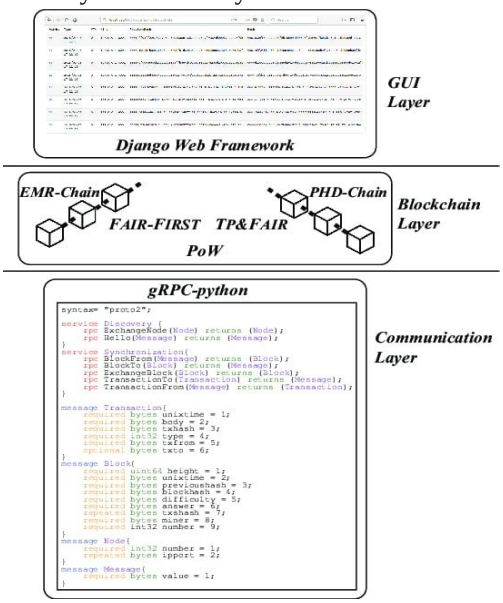


Fig 4:Level by level implementation

The bottom layer, i.e., communication layer, is imple-mented using gRPC-python1. There are two services to support Blockchain-based system, i.e., peer discovery service ("Dis-covery") and synchronization service ("Synchronization") as shown in Fig. 7. The "Discovery" service is used for dis-covering the nodes inside the Blockchain network. When a node is started, it will greet several static nodes (the same as bootnodes in Ethereum) and exchange the connectivity information with the static nodes. The block and transaction synchronization is achieved by the "Synchronization" service, which includes several remote procedure calls (RPCs) such as "BlockFrom", "BlockTo", "BlockFrom", "TransactionTo", and "TransactionFrom".

At the middle layer, two Blockchains, i.e., EMR-Chain and PHD-Chain are implemented. The EMR-Chain employs the FAIR-FIRST transaction packing algorithm while the PHD-Chain utilizes the TP&FAIR transaction packing algorithm.

Django web framework2 is used in the top layer, i.e., the GUI layer. It opens an HTTP port and presents HTML pages using the port. In this way, the users can submit data fol-lowing the HTTP protocol. When some data is submitted, we invoke the methods on Blockchain layer to fulfill Blockchain functions.

After implementation, we measure the performance of BlocHIE with 8 nodes. Each node is serving as both server and client, i.e., sending requests and packing transactions at the same time. The frequency of sending requests of each node is around 7 tx/s. Moreover, we set the number of transactions inside a block, i.e., m, to be 56, which is the approximate transaction generating rate. We compare the performance of TP&FAIR, FAIR-FIRST, and RANDOM concerning both fair-ness and throughput. Here, the RANDOM packing algorithm refers to the algorithm that randomly pick m transactions from pool. The result is shown in Fig. 8. We observe that in terms of fairness, both FAIR-FIRST and TP&FAIR outperform RANDOM significantly. Specifically, they achieve up to 2.9x and 2.6x higher fairness than RANDOM respectively. From the perspective of throughput, TP&FAIR achieves the maximum, i.e., 46 tx/s, which improves FAIR-FIRST over 23.6%.

IV. CONCLUSION

In this paper, we propose BlocHIE, a Blockchain-based platform for healthcare information exchange. We consider two kinds of healthcare data, i.e., electronic medical records and personal healthcare data, and analyzed the different re-quirements to store and share them. Based on the analysis, we architect BlocHIE on two loosely-coupled Blockchains, i.e., EMR-Chain for electronic medical records and PHD-Chain for personal healthcare data. Inside EMR-Chain, we integrate the techniques of off-chain storage and on-chain verification to take good care of privacy and authenticability. Moreover, we propose two transaction packing algorithms to enhance the system throughput and the fairness among users. Finally, the implementation and evaluation indicate the practicability and effectiveness of BlocHIE.

REFERENCES

[1] "Measuring the value of helath information exchange",in information exchnage by B.E Dixon
[2] "The Internet Of Things for health care:a comprehensive survey",by S.R.Islam,D.kwak
[3] "A new initiative on precision medicine" by F.S.collins and H.Varmus.
[4] "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems.",A.Lei,Y.Cao,C.P.A.ough
[5] Eductx: A blockchain-based higher education credit platform.",M. Turkanovic,´ M. Holbl,¨ K. Kosiˇc,ˇ M. Hericko,ˇ and A. Kamisaliˇc
[6] "The application of blockchain technology in e-government in china," H.Hou

[7] "Medshare: Trust-less medical data sharing among cloud service providers via blockchain,"Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani
[8] "On the design of a blockchain platform for clinical trial and precision medicine",Z. Shae