Privacy Preserving Universally Accessible Electronic Healthcare Record Sharing System using Blockchain

Ujjwal Ahamed Molla, MTech Project Presentation
Distributed Computing Lab, Dept. of CSA, IISc, Bangalore

1. Problem Statement

Existing EHR systems are associated with a specific healthcare organisation. It is not interoperable accross organisations and lacks the ability to easily share data among organisations while maintaining data privacy and confidentiality.

2. Challenges faced by existing EHR Systems

- Interoperability
- Databreach
- Information Asymmetry

3. EHR System Requirements

- Interoperability
- Security and Privacy
- Patient-powered EHR
- Efficiency
- Scalability
- Availability

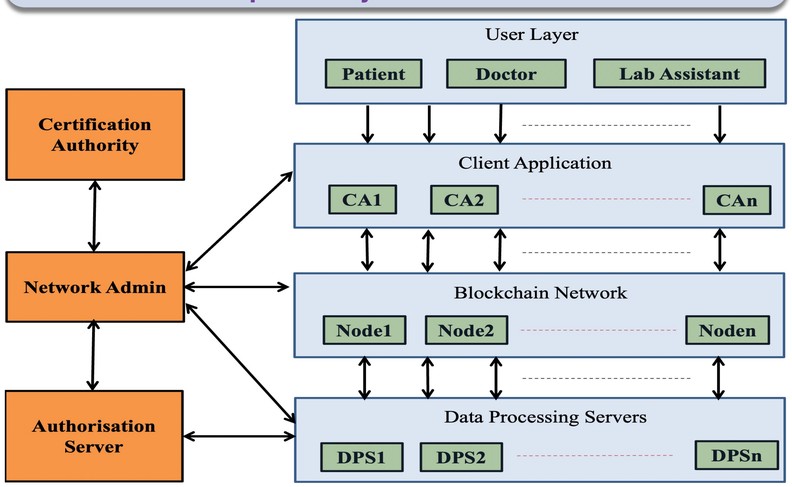
4. Why Blockchain

- Decentralized
- Transparent
- Immutable
- Secure

5. What We have Done

- Proposed a medical data sharing system based on permissioned blockchain.
- Used encryption-decryption technique to ensure medical data privacy, confidentiality, access control as well as data integrity.
- As data is stored in Blockchain, it is accessible to the authorised users from any organization.
- Our Solution preserves data privacy and confidentiality even from unauthorised participants of blockchain.
- Improved search technique using pointer.

6. Proposed System Archetecture



7. System Design

- Certification Authority : Provides certificate to network nodes and other units for identification and authentication purpose.
- Network Admin : Manages the network.
- Authorisation Server: Responsible for Key generation & management.
- Data Processing Servers : Responsible for data encryption-decryption with the help of Authorisation Server.
- Blockchain Network : Comprise of mutiple nodes and data are stored in encrypted form.
- Client Applications: Applications for the users to interact with the blockchain.
- Users : Patients, Doctors, Lab assistants etc.

8. Block Structure

Block Header

index : 4
previous_hash : "10a77e5000b9da11df154ac28c7aafc73dad8514d3a38fe16efe4a5d336544df"
Block_hash : 1eb9a51f806c6052cd3d06b58b7531a85fc865116d7320716473dc689a78f831"
timestamp : 1654628927.6448781

Transaction 1

sender : "30819f300d06092a864886f70d010101050003818d00308189028181 00df8d8a2c637XXXXXXXXXX",
patient_id : "zaid",
doctor_id : "roy",
hospital_id : "5000",
details : "34ed66d56b317a0219dc270896a25855988fda1994b6a68122a94c26e6cd9c3XXXXXXXXXXXXXX",
timestamp : "1654628985.059535"
Signature : "69bdb2ec628a8824b521f25f0473feb4e2882c5579e1ab73774dee2511dc60b3b5551XXXXXXXXX",
transaction_id : "TX64663540-e695-11ec-bb2e-121d94a1e0c0"
nonce : "aea1162c92bc6b25b03f6aff7c6cc8f0"
patient_pntr : {"t_index": 1, "b_index": 2},
doctor_pntr : { "t_index": 1, "b_index": 2}

9. Adding Records to the Blockchain

- N - Blockchain Node
- DP - Data Processing Server
- A - Authorisation Server
- C - Client Application
- Tx -Transaction Data Collectected from User through Client Application
- K_{nd} - Shared key between Blockchain Node and Data Processing Server
- K_{ad} - Shared key between Authorisation Server and Data Processing Server

1. $N -> DP$: $C1_{Tx} = E_{K_{nd}}(Tx)$
2. $DP -> A$: ask for K_{enc}
3. $A -> DP$: $K_{enc} = hash(\alpha||nonce)$
   $C_{enc} = E_{K_{ad}}(K_{enc})$
   $nonce$
4. $DP -> N$: $Tx = D_{K_{nd}}(C1_{Tx})$
   $K_{enc} = D_{K_{ad}}(C_{enc})$
   $C_{Tx} = E_{K_{enc}}(Tx)$

10. Retrieving Record from the Blockchain

- C_{Tx} -Encrypted Transaction Data Fetched from Blockchain

1. $N -> DP$: C_{Tx}, $nonce$
2. $DP -> A$: send $nonce$ and ask for K_{enc}
3. $A -> DP$: $K_{enc} = hash(\alpha||nonce)$
   $C_{enc} = E_{k_{ad}}(K_{enc})$
4. $DP -> N$: $K_{enc} = D_{K_{ad}}(C_{enc})$
   $Tx = D_{K_{enc}}(C1_{Tx})$
   $C1_{Tx} = E_{K_{nd}}(Tx)$
5. $N -> C$: $Tx = D_{K_{nd}}(C1_{Tx})$

11. Demo of implemented System

	Doctor	Hospital	Transaction Id	Medicine	Medical Tests	Comments	Created On
1	roy	5000	TXf5be9abe-e7e9-11ec-8b41-121d94a1e0c0	antibiotic	blood test	take rest.	2022-06-09 17:17:37.794181
2	roy	5000	TXeb25058e-e7e9-11ec-8b41-121d94a1e0c0	paracetemol	blood test	take rest	2022-06-09 17:17:20.010498
3	roy	5000	TX8fefa908-e7e9-11ec-9f70-121d94a1e0c0	dolo-365	Covid-19 RT-PCR	Isolate yourself. Eat healthy ...	2022-06-09 17:14:46.983367
4	roy	5000	TXe5d597fc-e7e8-11ec-9538-121d94a1e0c0	paracetemol	blood test	Bed rest.	2022-06-09 17:10:01.601566

Patient Fetches his own record

	Patient	Hospital	Transaction Id	Medicine	Medical Tests	Comments	Created On
1	zaid	5000	TXf5be9abe-e7e9-11ec-8b41-121d94a1e0c0	antibiotic	blood test	take rest.	2022-06-09 17:17:37.794181
2	zaid	5000	TXeb25058e-e7e9-11ec-8b41-121d94a1e0c0	paracetemol	blood test	take rest	2022-06-09 17:17:20.010498
3	naman	5000	TXb751a816-e7e9-11ec-9f70-121d94a1e0c0	dolo-365	Covid-19 RT-PCR	Isolate yourself. Eat healthy diet.	2022-06-09 17:15:53.060867
4	zaid	5000	TX8fefa908-e7e9-11ec-9f70-121d94a1e0c0	dolo-365	Covid-19 RT-PCR	Isolate yourself. Eat healthy diet.	2022-06-09 17:14:46.983367
5	naman	5000	TXfc3bfde2-e7e8-11ec-9538-121d94a1e0c0	thyronorm	TSH,T3,T4	Control diet.	2022-06-09 17:10:39.185208
6	zaid	5000	TXe5d597fc-e7e8-11ec-9538-121d94a1e0c0	paracetemol	blood test	Bed rest.	2022-06-09 17:10:01.601566

Transaction History of a Patient Fetched by a Specific Doctor (“Dr. roy”)

	Doctor	Hospital	Transaction Id	Medicine	Medical Tests	Comments	Created On
1	das	5001	TX62c5ff60-e7ec-11ec-af17-121d94a1e0c0	Restricted record!!!	Restricted record!!!	Restricted record!!!	Restricted record!!!
2	das	5001	TX5ea0c384-e7ec-11ec-af17-121d94a1e0c0	Restricted record!!!	Restricted record!!!	Restricted record!!!	Restricted record!!!
3	roy	5000	TXb751a816-e7e9-11ec-9f70-121d94a1e0c0	dolo-365	Covid-19 RT-PCR	Isolate yourself. Eat healthy diet.	2022-06-09 17:15:53.060867
4	das	5001	TX4fc59f36-e7e9-11ec-b5f1-121d94a1e0c0	Restricted record!!!	Restricted record!!!	Restricted record!!!	Restricted record!!!
5	roy	5000	TXfc3bfde2-e7e8-11ec-9538-121d94a1e0c0	thyronorm	TSH,T3,T4	Control diet.	2022-06-09 17:10:39.185208

Medical History of a Patient (“naman”) fetched by “Dr. roy”

	Doctor	Hospital	Transaction Id	Medicine	Medical Tests	Comments	Created On
1	das	5001	TX62c5ff60-e7ec-11ec-af17-121d94a1e0c0	Glimepiride 2mg	sugar test	diet control	2022-06-09 17:34:59.708207
2	das	5001	TX5ea0c384-e7ec-11ec-af17-121d94a1e0c0	Glimepiride 1mg	sugar test	diet control	2022-06-09 17:34:52.747067
3	roy	5000	TXb751a816-e7e9-11ec-9f70-121d94a1e0c0	dolo-365	Covid-19 RT-PCR	Isolate yourself. Eat healthy diet.	2022-06-09 17:15:53.060867
4	das	5001	TX4fc59f36-e7e9-11ec-b5f1-121d94a1e0c0	thyronorm 50	Repeat TSH	TSH level increased.Do ...	2022-06-09 17:12:59.335989
5	roy	5000	TXfc3bfde2-e7e8-11ec-9538-121d94a1e0c0	thyronorm	TSH,T3,T4	Control diet.	2022-06-09 17:10:39.185208

Medical History of Patient (“naman”) after granting permission to “Dr. roy”

References

1. Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid. Using blockchain for electronic health records. IEEE Access, 7:147782–147795, 2019.
2. Sudeep Tanwar, Karan Parekh, and Richard Evans. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applica- tions, 50:102407, 2020.
3. Guang Yang, Chunlei Li, and Kjell E Marstein. A blockchain-based architecture for securing electronic health record systems. Concurrency and Computation: Practice and Experience, 33(14):e5479, 2021.