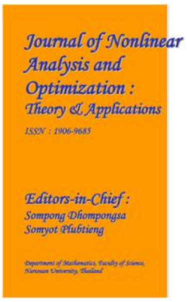
Journal of Nonlinear Analysis and Optimization
Vol. 12, No. 1, (2021),
ISSN : **1906-9685**



Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685
Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng
Department of Mathematics, Faculty of Science, Naresuan University, Thailand

E-HEALTH SYSTEMS BLOCK CHAIN BASED ON MOBILE CLOUD FOR SECURE EHR SHARING

[1]Nakka Maisaiah, [2]Malabootula Mahesh Kumar, [3]Venkata Pradeep Kumar Jonna, [4]Gaddam Bhavana
[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Information Technology, Rishi MS Institute of Engineering and Technology for Women, Kukatpally, Hyderabad

ABSTRACT

Electronic health records (EHRs) are increasingly being stored in mobile cloud environments, which merge mobile technology with cloud computing to make it easier for patients and healthcare professionals to share medical data. With the help of this cutting-edge paradigm, healthcare services may be provided at minimal operational costs with a great degree of flexibility. This new paradigm does, however, bring up issues with network security and data privacy for e-health systems. It is a difficult problem to properly exchange EHRs across mobile users while ensuring high security levels in the mobile cloud. Using a mobile cloud platform and the decentralized interplanetary file system (IPFS), we provide a unique EHRs sharing structure in this study. In particular, we provide a reliable access control system utilizing smart contracts to accomplish secure EHRs sharing among different patients and medical providers. Wepresent a prototype implementation using Ethereum block chain in a real data sharing scenario on a mobile app with Amazon cloud computing. The empirical results show that our proposal provides an effective solution for reliable data exchanges onmobile clouds while preserving sensitive health information against potential threats. The system evaluation and security analysis also demonstrate the performance improvements in lightweight access control design, minimum network latencywith high security and data privacy levels, comparedto the existing data sharing models.

EXISTING SYSTEM

Blockchain is a paradigm-shifting technology that has emerged over the past decade, which is based on peer-to-peercommunication technology, network theory, and crypto graphy .However, there are still some limitations in the existing blockchain framework that prevents its widespread adoptionin the commercial world. One important limitation is the storage requirement, whereineach blockchain node has to store a copy of the distributed ledger. •us, as the number of transactions increases, this storage requirement grows quadratically, eventually limiting thescalability of a blockchain system.

Disadvantages of Existing System:

1. More security issues.

PROPOSED SYSTEM

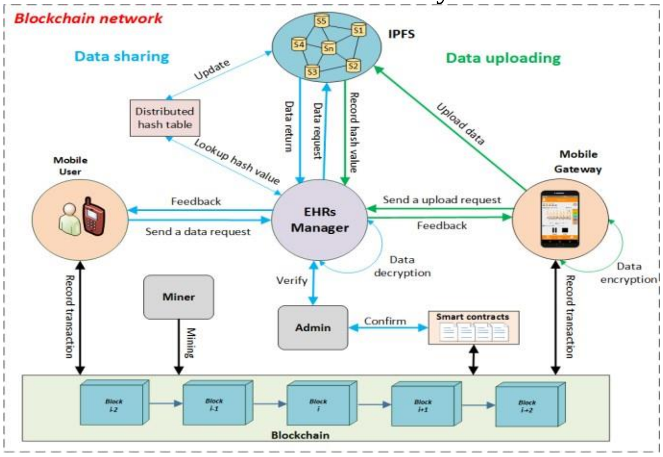
In this paper, instead of saving entiretransaction of blocks we are saving only oneblock. To provide security to block author converting that block in to SHAMIR share and then all SHAMIR share will be distributed between all available nodes.While reconstruction application will obtain all shares from nodes and then apply SHAMIR SECRET to recover original blockdata. If any share missed or return incorrect value then reconstruction will be failed.SHAMIR secret will work based on random polynomial and prime number whilegenerating secret polynomial will be appliedon block data and while getting original value will perform reverse polynomial.

http://doi.org/10.36893/JNAO.2021.V12I1.089-093

SYSTEM MODEL

In this section, we present a system architecture and introduce the concept of data uploading and data sharing in our system. Further, design goals in this paper are also highlighted. FIGURE 1. The overview of blockchain based e-health system on mobile cloud. FIGURE 2. Thedata flow of the proposed mobile cloud blockchain system.

FIGURE 1. The overview of blockchain based e-healthsystem on mobile cloud.



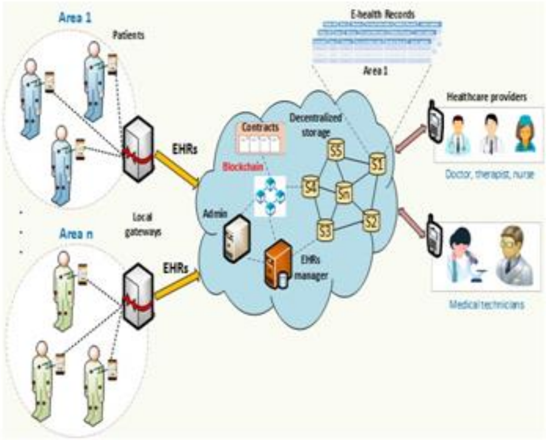


FIGURE 2. The data flow of the proposed mobile cloudblockchain system.

A. SYSTEM ARCHITECTURE We consider an e-health scenario on amobile cloud platform where patientrecords are gathered from a network oflocal gateways and stored on a publiccloud for sharing with healthcareproviders as shown in Fig. 1. E-healthrecords may include personalinformation and medical history whichare provided by patients. Patients havetheir own patient ID PID and areclassified based on their current livingarea with an area ID AID. In this model,we assume that the wearable sensornetwork is private and managed by its local user (patient). We also assume thatEHRs can be collected from wearable body sensors by a mobile applicationintegrated in patients' smartphone.Therefore, the address of a patient on blockchain can be formulated as Addr = {AID, PID}. Because it is infeasible to store medical data on blockchain, we suggest to only keep addresses of patients on blockchain, while large medical records are stored on decentralized cloud storage. Further, to manage medical records, a cloud EHRs manager ME is proposed. Thus, in orderto retrieve a certain health record on cloud, a participating entity needs to know patient addresses which are visible on the blockchain network. The data flow of the proposed mobile cloud blockchain system is also shown in Fig. 2.

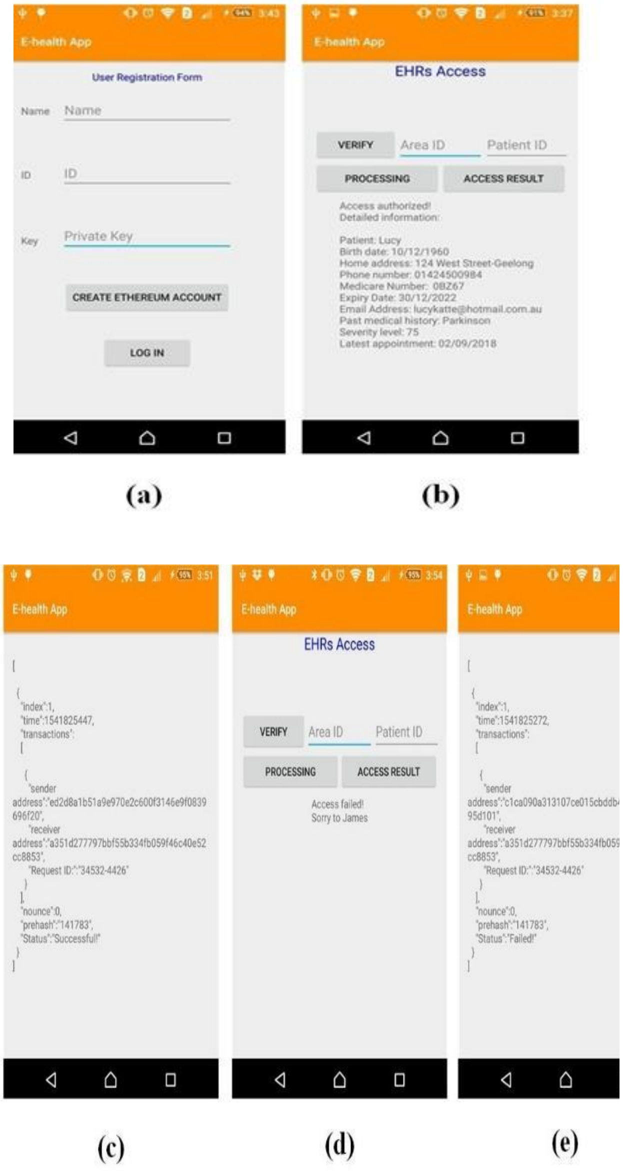
EXPERIMENTAL RESULTS

To implement our EHRs sharing framework,we first deployed a private Ethereumblockchain on AWS as illustrated in Fig. 11.Data access and transactions are recorded and shown on the web interface formonitoring. Based on blockchain settings,we deployed smart contracts, IPFS storage, established network entities and connected with mobile applications to build our e- health framework. With these settings, weoperated the EHRs sharing system andevaluated the efficiency of our designthrough two main performance metrics:access control and network overheads.

ACCESSCONTROLPERFORMANCE

We present two use cases with authorized and unauthorized access to evaluate the performance of our EHRs sharing model with a designed access control (Fig. 12). Theobjective of our framework is to allow authorized entities (such as healthcare providers) to retrieve effectively EHRs on cloud, while being able to prevent unauthorized access to our EHRs resources. A mobile user such as a doctor, who wants to access EHRs of his patient on cloud, can use our mobile application with a mobileuser interface to create an Ethereum

account and register user information for interacting with the blockchain (Fig. 12(a)). After his request is verified by the cloudEHRs manager, he now starts to make a transaction to access EHRs by providing the address of his patient



Access authorized!
Detailed information:

Patient: Lucy
Birth date: 10/12/1960
Home address: 124 West Street-Geelong
Phone number: 01424500984
Medicare Number: 08Z67
Expiry Date: 30/12/2022
Email Address: lucykatte@hotmail.com.au
Past medical history: Parkinson
Severity level: 75
Latest appointment: 02/09/2018

(a) (b)

```
[
 {
  "index":1,
  "time":1541825447,
  "transactions":
  [
   {
    "sender
address":"ed2d8a1b51a9e970e2c600f3146e9f0839
696f20",
    "receiver
address":"a351d277797bbf55b334fb059f46c40e52
cc8853",
    "Request ID:":"34532-4426"
   }
  ],
  "nounce":0,
  "prehash":"141783",
  "Status":"Successful!"
 }
]
```

Access failed!
Sorry to James

```
[
 {
  "index":1,
  "time":1541825272,
  "transactions":
  [
   {
    "sender
address":"c1ca090a313107ce015cbddb
95d101",
    "receiver
address":"a351d277797bbf55b334fb059
cc8853",
    "Request ID:":"34532-4426"
   }
  ],
  "nounce":0,
  "prehash":"141783",
  "Status":"Failed!"
 }
]
```

(c) (d) (e)

Advantages of Proposed System:

1. This can effectively work.
2. Security is more.

REQUIREMENT SPECIFICATION

Functional Requirements

- Graphical User interface withthe User. Software Requirements

For developing the application the following are the Software Requirements:

1. Python
2. Django
3. Mysql
4. Wampserver(Mysql)

Operating Systems supported

1. Windows 7
2. Windows XP
3. Windows 8/10/11

Technologies and Languages used to Develop

1. Python

Debugger and Emulator

- Any Browser (ParticularlyChrome)

CONCLUSION

This paper proposes a novel EHRs sharing scheme enabled by mobile cloud computing and blockchain. We identify critical challenges of current EHRs sharing systems and propose efficient solutions to addressthese issues through a real prototype implementation. In this work, our focus is on designing a trustworthy access controlmechanism based on a single smart contract to manage user access for ensuring efficient and secure EHRs sharing. To investigate the performance of the proposed approach, we deploy an Ethereum blockchain on theAmazon cloud, where medical entities can interact with the EHRs sharing system via a developed mobile Android application. We also integrate the peer-to-peer IPFS storage system with blockchain to achieve a decentralized data storage and data sharing. The implementation results show that ourframework can allow medical users to share medical data over mobile cloud environments in a reliable and quick manner

, in comparison to conventional schemes. In particular, our access control can identifyand prevent effectively unauthorized access to the e-health system, aiming for achievinga desired level of patient privacy and network security. We also provide security analysis and extensive evaluations onvarious technical aspects of the proposed system, showing advantages of our proposal over existing solutions. Based on the merits of our model, we believe that our blockchainenabled solution is a step towards efficient management of e-health records on mobile clouds, which is promising in many healthcare applications.

REFERENCES

1. T.-T. Kuo, H.-E. Kim, and L. Ohno- Machado, ``Blockchain distributed ledger technologies for biomedical andhealth care applications," J. Amer. Med. Inf. Assoc., vol. 24, no. 6, pp.1211_1220, 2017.

2. M. Mettler, ``Blockchain technology inhealthcare: The revolution starts here," in Proc. 18th IEEE Int. Conf e-HealthNet., Appl. Services, Sep. 2016, pp. 1_3.

3. W. J. Gordon and C. Catalini, ``Blockchain technology for healthcare: Facilitating the transition to patient-driveninteroperability," Comput. Struct. Biotechnol J., vol. 16, pp. 224_230, 2018.

4. A. Dubovitskaya, Z. Xu, S. Ryu, M.Schumacher, and F. Wang, ``Secure and trustable electronic medical recordssharing using blockchain," in Proc. AMIA Annu. Symp., 2017, pp.650_659.

5. M. Hölbl, M. Kompara, A. Kami²alic,and L. N. Zlatolas, ``A systematic review of the use of blockchain inhealthcare," Symmetry, vol. 10, no. 10, p. 470, 2018.

6. S. Jiang, J. Cao, H. Wu, Y. Yang, M.Ma, and J. He, ``BlocHIE: A blockchain-based platform

for healthcareinformation exchange,'' in Proc.IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun. 2018, pp. 49_56.
7. L. A. Tawalbeh, R. Mehmood, E.Benkhlifa, and H. Song, ``Mobile cloud computing model and big data analysis forhealthcare applications,'' IEEE Access, vol. 4, pp. 6171_6180, 2016.
8. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, ``The Internet of Things forhealth care: A comprehensive survey,'' IEEE Access, vol. 3, pp. 678_708,Jun. 2015.
9. Bahga and V. K. Madisetti, ``Acloud-based approach for interoperable electronic health records (EHRs),'' IEEE J.Biomed. Health Inform., vol. 17, no. 5, pp. 894_906, Sep. 2013.
10. E. AbuKhousa, N. Mohamed, and J. Al- Jaroodi, ``e-Health cloud: Opportunities and challenges,'' Future Internet, vol. 4, no.3, pp. 621_645, 2012.

http://doi.org/10.36893/JNAO.2021.V12I1.089-093