INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Securing Healthcare Data in Blockchain Using TSE Algorithm

P Arul[1], S Renuka[2]*

1 Research Supervisor, Assistant Professor, Department of Computer Science, Government Arts College (Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli, 620 022, Tamil Nadu, India
2 Assistant Professor, Department of Computer Science, Government Arts College (Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli, 620 022, Tamil Nadu, India

OPEN ACCESS

Received: 19-07-2023

Accepted: 29-09-2023

Published: 17-11-2023

Citation: Arul P, Renuka S (2023) Securing Healthcare Data in Blockchain Using TSE Algorithm. Indian Journal of Science and Technology 16(43): 3942-3947. https://doi.org/10.17485/IJST/v16i43.1815

* **Corresponding author**.

spkumarrenu@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: The main objective of this work is to create a novel patient-centered management system that uses the two-stage encryption TSE algorithm to secure a private blockchain-based healthcare system while providing users with the highest privacy, complete control, and security over their sensitive data. **Methods:** TSE Encryption Process: The user or the patient asymmetrically encrypts the data's symmetric key using the public key of the party with whom the data is to be shared. TSE Decryption Process: The party wishing to access the health data initially selects the user (patient), then sends the private key to decrypt the data present in the network. The public key of the user is used to verify the signature, and finally, the confidential data is retrieved back to be accessed by the party intended to see it. The TSE algorithm is compared to the DES (Data Encryption Standard) and MD5 (Message Digest Method 5) algorithms, and the results show that the proposed algorithm performed significantly better than the other two. **Finding:** In this work, the asset is encrypted and indexed in a database, and the asset's value or data is encrypted and stored on a private blockchain to provide the best possible privacy and security. The concept makes use of the immutability, cryptography, and distribution aspects of the blockchain but overlooks the blockchain's public nature and the conventional mining process. **Novelty:** Most existing approaches store all of the data in the blockchain, which reduces user privacy. The proposed algorithm uses the blockchain to store the index of the health care asset.

Keywords: Blockchain; Healthcare; Privacy; cryptography; and Two Stage Encryption (TSE) algorithm

1 Introduction

The volume of digital health data available today is expanding rapidly, creating what is known as healthcare data (HD). This fact is directly related to the development of smart phones, Internet of Things (IoT) gadgets, software applications, and the digitization of patient and clinical information. Like other forms of big data, HD can be highly useful and important. This HD information can help us understand the disease better, reduce the overall supply chain cost of the medicines, and finally improve the quality of life for each and every person on earth.

Blockchain in healthcare faces challenges that need to be resolved. The first problem has to do with confidentiality and openness[1]. Transparency may be one of the most significant benefits of blockchain technology because it increases user confidence. However, if ”smart contracts” are not properly implemented to handle permissions, it can be problematic for the privacy of the patients and users since the metadata that comes with information is visible and transparent to all users in a blockchain network, which hinders the privacy of the patients.

The second most important problem is the ”pseudonymity”[2] of the users, as the technology identifies the user by hash values that are not easy to examine. The next important challenge is the scalability of the blockchain if all the healthcare data is stored in the blocks; it is not easy to achieve the desired speed.

The solution to address the aforementioned problem is to use the blockchain to store only the index of the data and to store the original raw data in a data pool. Each and every piece of data inside the block would have a user hash value[3] and a raw healthcare data link in encrypted format, where the encrypted link acts as a pointer to the actual data that is being stored in the data pool. The data pool is a collection of data repositories where the actual clinical healthcare data is stored in encrypted format and a corresponding index value is generated for each record to be put into the blockchain. A plethora of information related to prescriptions, blood types, pressure, sugar levels, pulse rate scan reports, doctors, and lab reports is archived in the data pools, which are indexed with the pointer on the blockchain.

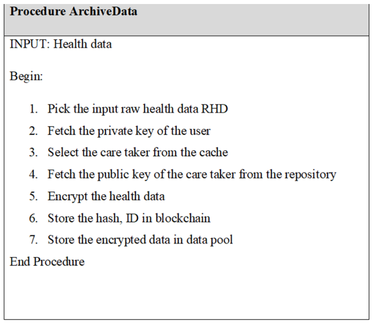
2 Methodology

2.1 Proposed approach

The network that is being used for the implementation of the blockchain is a private one, and the network can be accessed only by the users and the medical expert or caretaker of the patient. In this paper, the dual encryption key process of public key and private key is used. In order to do this, the RSA algorithm is being implemented with caution to ensure patient data and privacy[4]. All the public keys that are being generated are stored in the repository. This public and private key pair plays a pivotal role in the encryption and decryption of the healthcare data that is stored in the blockchain and data pool[5].

The data is initially encrypted using a symmetric algorithm, and then the key is asymmetrically encrypted to ensure that the authorized person can access the user’s data using the symmetric public key[6]. The asymmetric encryption is processed using the public key of the caretaker, and it will be stored in the repository. Also, the confidential data will be digitally signed[7] using the private key of the user for security. The data is encrypted and signed before being uploaded to the blockchain network.

The stored data consists of two parts, namely the open and secret components. The open component is anonymous and contains only the hashes and the IDs of the data, which are public and visible to everyone. The main goal of this part is to maintain the immutability and transparency of the ledger data. The secret part is the encrypted health data, which is accessible only to the owner and the authorized person with the signature. The caretaker public key is fetched from the repository to encrypt the confidential data, and then the encrypted data is stored in the blockchain and data pool where the actual raw data is archived. This data pool is not accessible by everyone, whereas only authorized persons who are authenticated by the user can be allowed to access the private data of the patients/users. The pseudocode of the data storage is shown in the following Figure 1.



```
Procedure ArchiveData
INPUT: Health data
Begin:
    1. Pick the input raw health data RHD
    2. Fetch the private key of the user
    3. Select the care taker from the cache
    4. Fetch the public key of the care taker from the repository
    5. Encrypt the health data
    6. Store the hash, ID in blockchain
    7. Store the encrypted data in data pool
End Procedure
```

Fig 1. Pseudo code to store health data

2.2 Retrieving the data

A particular user chooses the caretakers with whom to share confidential health data when he enters it into the blockchain. In doing so, the user or the patient asymmetrically encrypts the data's symmetric key using the other party's public key, with whom the data is to be shared or permitted to be shared. Hence, for every piece of health data, there will be a list of users with whom this confidential data has to be shared. The party can access the confidential data if their name is on the list provided in the repository. The party's private key will use the asset's symmetric key to unlock it, and that key will unlock the healthcare data. This data is then stored in the local cache of the caretaker. The party seeking access to the health data first chooses the user, and then sends the private key to decrypt the data already present in the network. The user's public key is then used to confirm the signature, and lastly, the private data is retrieved back to be accessed by the party intended to see it. The block diagram of the process is shown in Figure 2, and the pseudocode is shown in Figure 3.

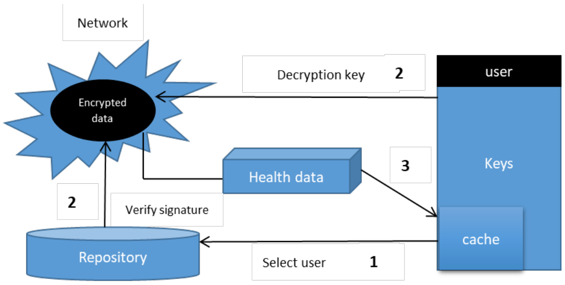
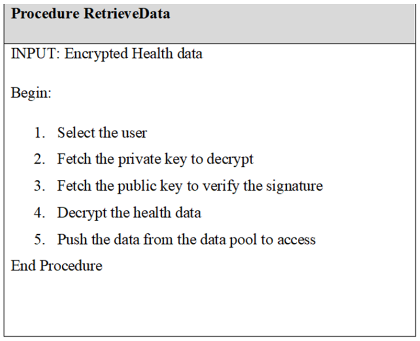


Fig 2. Pseudo code to retrieve health data



```
Procedure RetrieveData
INPUT: Encrypted Health data
Begin:
    1. Select the user
    2. Fetch the private key to decrypt
    3. Fetch the public key to verify the signature
    4. Decrypt the health data
    5. Push the data from the data pool to access
End Procedure
```

Fig 3. Pseudo code to retrieve the data

The entire process is twice encrypted using the two stage encryption algorithm TSE which is shown in Figures 4, 5, 6 and 7 in the following section along with the pseudocode. The sample data is shown in the Figure 8. The data is initially encrypted using the symmetric algorithm, and then this symmetric key is asymmetrically encrypted for the second time for additional security.

2.3 Sample block in the network

3 Results and Discussion

The proposed algorithm, along with the DES and MD5 algorithms, is implemented in Python, and the results are compared with respect to speed, power consumption, efficiency, and security. The following Figure 9 make it evident that the proposed algorithm is far better than the other two.

The Figure 10 clearly shows that the proposed TSE is better than the other two encryption methods, mainly due to its dual encryption scheme and proposed algorithm, which uses the blockchain only to store the index of the health care asset, whereas most of the existing methods store the entire data in the blockchain, which in turn reduces the privacy of the users (patients). It is demonstrated that by encrypting this model with fully homomorphism encryption and using the zero knowledge proof

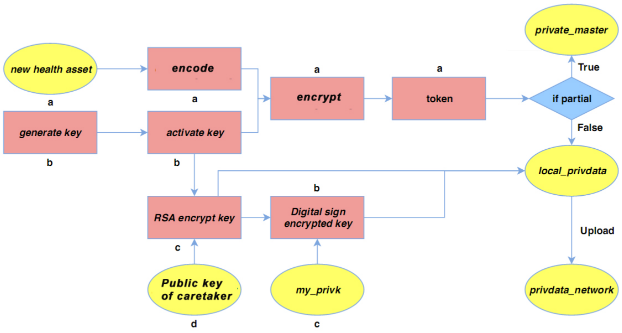
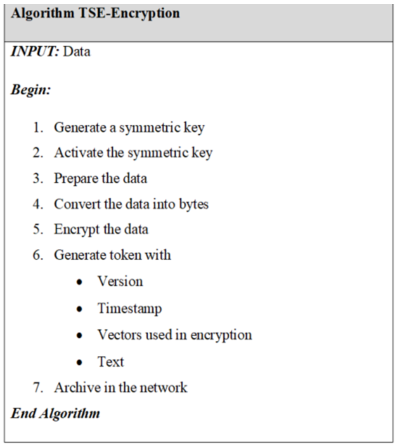


Fig 4. Two Stage TSE – Encryption process



```
Algorithm TSE-Encryption
INPUT: Data
Begin:
    1. Generate a symmetric key
    2. Activate the symmetric key
    3. Prepare the data
    4. Convert the data into bytes
    5. Encrypt the data
    6. Generate token with
        • Version
        • Timestamp
        • Vectors used in encryption
        • Text
    7. Archive in the network
End Algorithm
```

Fig 5. Pseudo code of TSE-Encryption

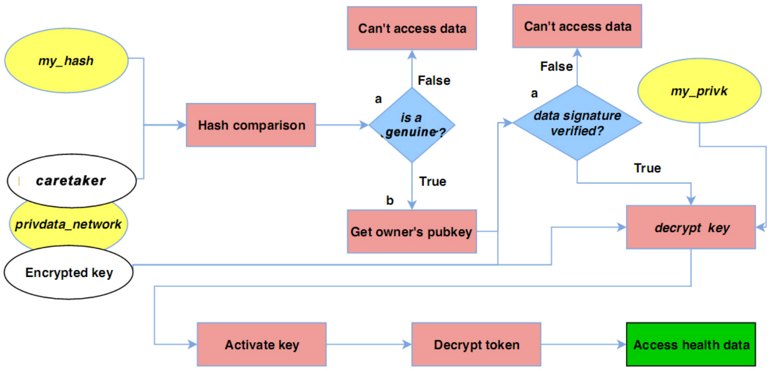
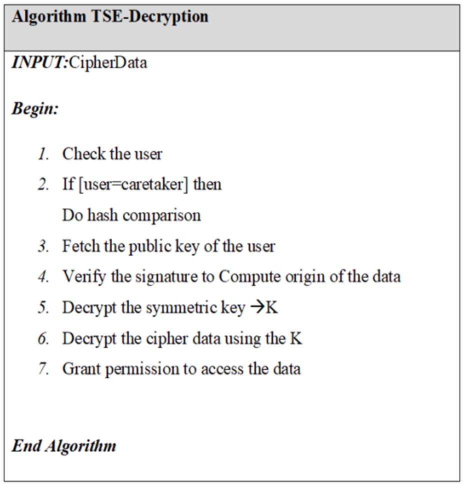
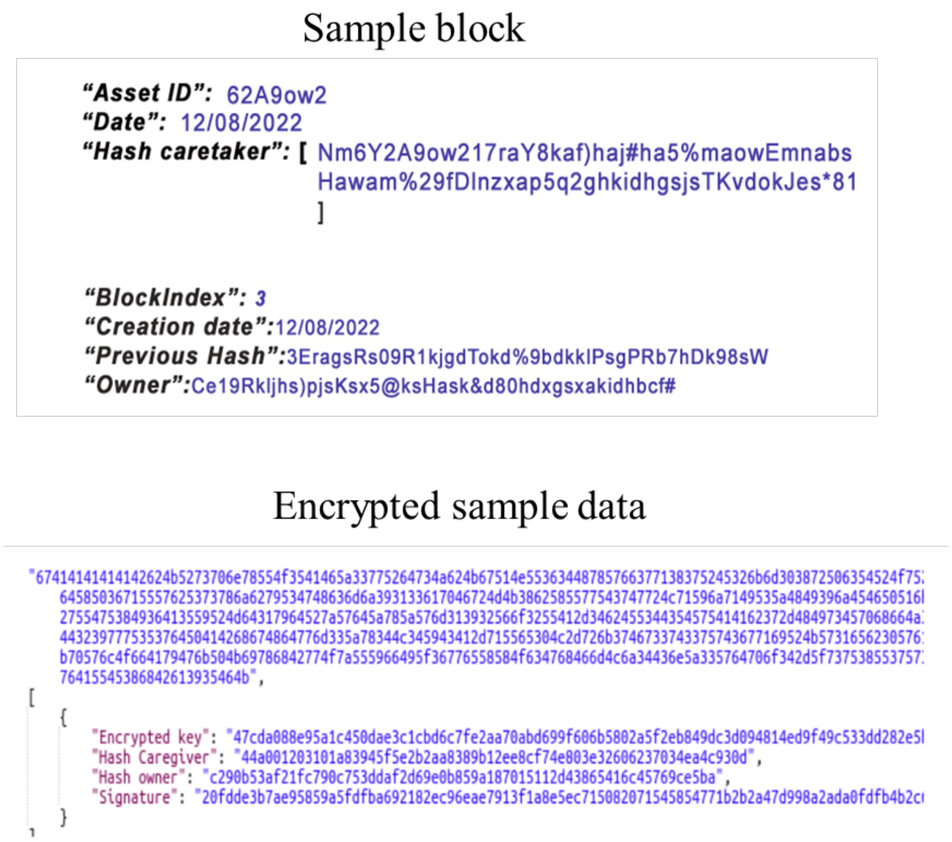


Fig 6. TSE – Decryption process



```
Algorithm TSE-Decryption
INPUT:CipherData
Begin:
    1. Check the user
    2. If [user=caretaker] then
       Do hash comparison
    3. Fetch the public key of the user
    4. Verify the signature to Compute origin of the data
    5. Decrypt the symmetric key →K
    6. Decrypt the cipher data using the K
    7. Grant permission to access the data
End Algorithm
```

Fig 7. Pseudo code of the TSE-Decryption algorithm



Sample block

“Asset ID”: 62A9ow2
“Date”: 12/08/2022
“Hash caretaker”: [Nm6Y2A9ow217raY8kaf)haj#ha5%maowEmnabs
Hawam%29fDInzxap5q2ghkidhgsjsTKvdokJes*81
]

“BlockIndex”: 3
“Creation date”:12/08/2022
“Previous Hash”:3EragsRs09R1kjgdTokd%9bdkkIPsgPRb7hDk98sW
“Owner”:Ce19Rkljhs)pjsKsx5@ksHask&d80hdxgsxakidhbcf#

Encrypted sample data

```
"674141414141142624b5273706e78554f3541465a33775264734a624b67514e5536344878576637713837524532 6b6d303872506354524f75
    645850367155576253737 86a62795347486 36d6a393133617046724d4b386258557754374772 4c71596a7149535a4849396a454650516
    275547538493641355952 4d64317964527a57645a785a576d313932566f3255412d346245534435457541416237 2d484973457068664a
    443239777535376450414268674864776d335a78344c345943412d715565304c2d726b3746733743375743677169524b573165623057 6
    b70576c4f664179476b504b69786842774f7a555966495f36776558584f634768466d4c6a34436e5a335764706f342d5f737538553757
    7641554538684261393546 4b",
[
    {
        "Encrypted key": "47cda088e95a1c450dae3c1cbd6c7fe2aa70abd699f606b5802a5f2eb849dc3d094814ed9f49c533dd282e5
        "Hash Caregiver": "44a001203101a83945f5e2b2aa8389b12ee8cf74e803e32606237034ea4c930d",
        "Hash owner": "c290b53af21fc790c753ddaf2d69e0b859a187015112d43865416c45769ce5ba",
        "Signature": "20fdde3b7ae95859a5fdfba692182ec96eae7913f1a8e5ec71508207154585 4771b2b2a47d998a2ada0fdfb4b2c
    }
]
```

Fig 8. Sample encrypted data

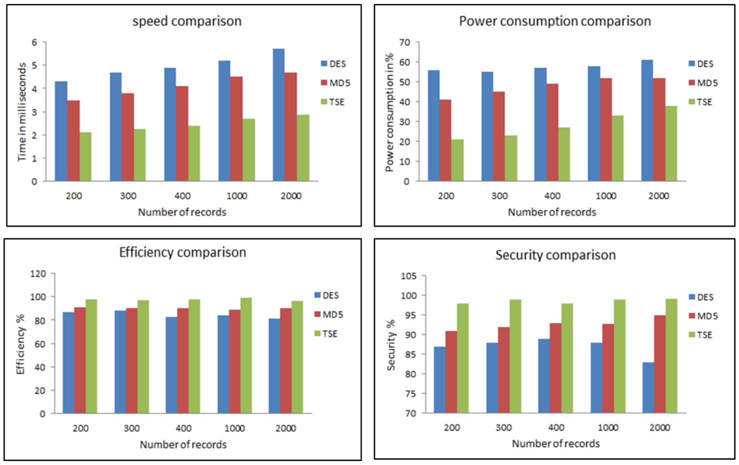


Fig 9. Comparison charts

of unencrypted understanding, the traceability and balance of the permissioned blockchain can be demonstrated with zero knowledge of the permission less blockchain while the risk tolerance of the permissioned blockchain is hidden.

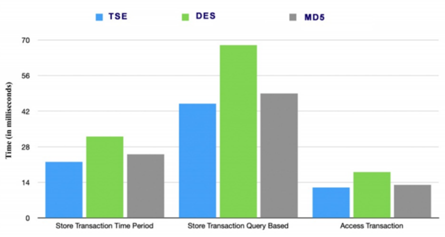


Fig 10. Transaction time comparison

4 Conclusion

This research created a hybrid blockchain model to store and share private and sensitive health data with highly enhanced security and privacy. This concept uses the blockchain's immutability, cryptography, and distribution features but ignores the public nature of the blockchain and the conventional mining process.

References

1) Peng L, Feng W, Yan Z, Li Y, Zhou X, Shimizu S. Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*. 2021;7(3):295–307. Available from: https://doi.org/10.1016/j.dcan.2020.05.008.
2) Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*. 2020;97:1–20. Available from: https://doi.org/10.1016/j.cose.2020.101966.
3) Shahidehpour M, Yan M, Shikhar P, Bahramirad S, Paaso A. Blockchain for Peer-to-Peer Transactive Energy Trading in Networked Microgrids: Providing an Effective and Decentralized Strategy. *IEEE Electrification Magazine* . 2020;8(4):80–90. Available from: https://doi.org/10.1109/MELE.2020.3026444.
4) Nidhya R, Shanthi S, Kumar M. A Novel Encryption Design for Wireless Body Area Network in Remote Healthcare System Using Enhanced RSA Algorithm. In: Intelligent System Design;vol. 1171 of Advances in Intelligent Systems and Computing. 2020;p. 255–263. Available from: https://doi.org/10.1007/978-981-15-5400-1_27.
5) Huang H, Sun X, Xiao F, Zhu P, Wang W. Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. *Journal of Parallel and Distributed Computing*. 2021;148:46–57. Available from: https://doi.org/10.1016/j.jpdc.2020.10.002.
6) Zhai S, Yang Y, Li J, Qiu C, Zhao J. Research on the Application of Cryptography on the Blockchain. *Journal of Physics: Conference Series*. 2019;1168(3):1–8. Available from: https://doi.org/10.1088/1742-6596/1168/3/032077.
7) Fang W, Chen W, Zhang W, Pei J, Gao W, Wang G. Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*. 2020;(56):1–15. Available from: https://doi.org/10.1186/s13638-020-01665-w.