Computers, Materials & Continua
DOI: 10.32604/cmc.2022.029538
Article

Tech Science Press

Enhancing Blockchain Security Using Ripple Consensus Algorithm

A. Baseera[1] and Abeer Abdullah Alsadhan[2,*]

[1]School of Computing Science and Engineering, VIT Bhopal University, Bhopal, 466114, India
[2]Department of Computer Science, Imam Abdulrahman Bin Faisal University, Dammam, 34212, Saudi Arabia
*Corresponding Author: Abeer Abdullah Alsadhan. Email: abeerabdullah2@outlook.com
Received: 06 March 2022; Accepted: 21 April 2022

Abstract: In the development of technology in various fields like big data analysis, data mining, big data, cloud computing, and blockchain technology, security become more constrained. Blockchain is used in providing security by encrypting the sharing of information. Blockchain is applied in the peer-to-peer (P2P) network and it has a decentralized ledger. Providing security against unauthorized breaches in the distributed network is required. To detect unauthorized breaches, there are numerous techniques were developed and those techniques are inefficient and have poor data integrity. Hence, a novel technique needs to be implemented to tackle the new breaches in the distributed network. This paper, proposed a hybrid technique of two fish with a ripple consensus algorithm (TF-RC). To improve the detection time and security, this paper uses efficient transmission of data in the distributed network. The experimental analysis of TF-RC by using the metric measures of performance in terms of latency, throughput, energy efficiency and it produced better performance.

Keywords: Blockchain; security; ripple; breaches; twofish; network

1 Introduction

In today's world, everything is connected with IoT based on the environment. For transmission of data or sharing of information through the network, security plays an important role. Cloud storage offers unlimited storage for computing resources and information by using multiple users [1]. Blockchain technology is one of the models for providing a high level of security based on the concept of cryptographic mechanisms in the decentralized approach which replaces various existing implementations of security. In blockchain technology, the chain of blocks in each block contains information or data which are available in a distributed ledger. It is a software protocol and it could not be implemented without the internet which comprises software applications, databases, and interconnecting various computers [2].

Rivest-Shamir-Adleman (RSA) is one of the cryptographic keys, and it is used to store information as records. The cryptographic technique for encrypting the data using a private key which is different from a decryption key? The concept of Rivest Shamir Adleman (RSA) is asymmetry centric based on

the positive product of integer values as a "factoring issue" [3]. In the decentralized-based network, Blockchain allows registering a sequence of transformations potentially despite doing a malicious activity in the minority of peer-to-peer (P2P). Blockchain activities revolutionize different fields like currency-based systems, and payment in the financial sectors which are automatically employed contracts in IoT of massive sharing of data [4–8].

Many research works have been done and applying these techniques and will be insecure and inefficient in the detection of breaches. Therefore, to improve the security and detection of malicious or breaches activities this paper proposed Two fish-based Ripple Consensus algorithms (TF-RC). This TF-RC uses RSA for the authentic registration process and in blockchain technology uses a ripple consensus algorithm. The main contribution of this work is:

1. A novelty and trusted cloud-based system with the implementation of a blockchain using the RSA mechanism will improve the sharing of data overhead by maximizing energy efficiency.
2. Enhancing the security in blockchain technology using a ripple consensus algorithm.

The paper has been organized as follows: Section 2 describes the review of the literature, Section 3 introduces enhancing the blockchain security using the ripple consensus algorithm, Section 4 discusses the experimented results and Section 5 concludes the paper with future directions.

2 Review of Literature

In the modern world, sharing information through the network is essential in preserving the information secure manner. Blockchain is a type of distributed ledger method [9]. Blockchain technology is implemented in the field of bitcoin, cryptocurrency, Monroe, Litecoin, and Zcash [10–12]. The rapid development of the blockchain method can efficiently in providing the reliability, authenticity, and security of information. It is also used in the protection of personal data, preserving data, and allocation of data [13–15]. The smallest unit of blockchain is a block. Each block contains a header, data, and body of blocks which is mainly used for the transmission of data. The transformation of data is done by using a hash function, and it provides security in the blockchain [16].

This paper [17] proposed the contribution of the infrastructure of cloud storage like private clouds and public clouds. Accessing information or data is controlled by registered users in a secure and it is employed in the cloud service provider. The standard encryption scheme used the term frequency-inverse document frequency (TF-IDF) technique which is used in the link of semantic documents and keywords. To ensure security and keep the privacy-preserving by using the encryption scheme of Latent Dirichlet Allocation (LDA). In the LDA, the document is created based on the concept-wise and the relevant matrix with vector query. To improve the efficiency of this implementation of the LDA method by using the "Greedy Depth First Search" algorithm [18].

The paper [19] proposed the transformation of data or information in the P2P network model. In blockchain technology proof of production and stack proof are used in the blockchain credibility. The blockchain concept focused on private provable data possession (PDP) recognizes the security of the customer in the terms of anonymity. For boosting efficiency, it is necessary to discard the certificate authentication technique. In the PDP concept, the blockchain-based analysis uses the private key which provides the information more secure. The various consensus algorithms in blockchain technology are Ripple, decentralized autonomous organization (DAC), proof of stack (PoS), proof of activity (PoA), and proofof work (PoW) [20,21].

Tab. 1 shows the literature survey of block chain.

Table 1: Shows that survey on blockchain technology in storing data more secure way

Author name	Description of technique used
AbuElezz et al. [22]	New lightweight cryptographic algorithm. It consists of 16 bytes (128-bit) block cipher and is used to encrypt the data.
Liu et al. [23]	It is based on the hybrid technique of HW/SW architecture for Proof of Work (PoW) consensus. It uses the Ethereum blockchain with the Keccak 256 and the field-programmable gate array (FPGA) ZedBoard development kit.
Ismail et al. [24]	The hybrid adaptive crypto cloud framework by combining blockchain technology and botnet
Wang et al. [25]	To encrypt the data, and provide an effective privacy protection technique called Elliptic Curve Cryptography (ECC)
Sun et al. [26]	To enhance privacy by preserving the distributed protocol for data aggregation based on blockchain and homomorphic encryption
Anjana et al. [27]	Adaptive light weight encryption algorithm for securing multi-cloud storage
Jabeen et al. [28]	Detection of threats in blockchain

3 Proposed Methodology

Storing and sharing data or information using blockchain technology requires security in breaches and reliability of data transactions in the distributed network. The system model of storage of data based on blockchain with the cloud is shown in Fig. 1.

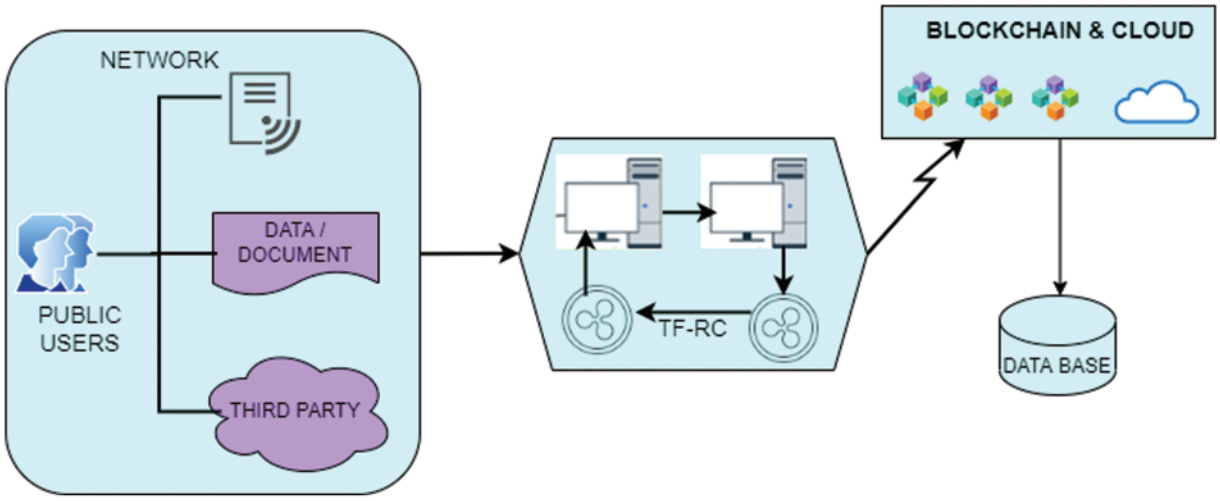

Figure 1: Blockchain-based cloud storage

Fig. 1 describes the blockchain architecture for storing information in high-level security. This proposed work (TF-RC) contains two modules.

Module 1: Registration for user and Verification

Module 2: Data Storage securely using TF-RC

Module 3: Updating Authentic information

Module 4: Detection of Breaches in the distributed network

3.1 Registration Form User and Verification

In this module, the user will do the registration procedure with a certificate authority. Every successfully registered user receives the key for encrypted data. By using the credentials registered users can enter into the system. The credential information contains the id, password, and random key number for the verification. If the verification details are valid then the authentication is granted to the user, otherwise, it will be rejected. The RSA algorithm is implemented for verification. Fig. 2 shows the workflow of the RSA algorithm.

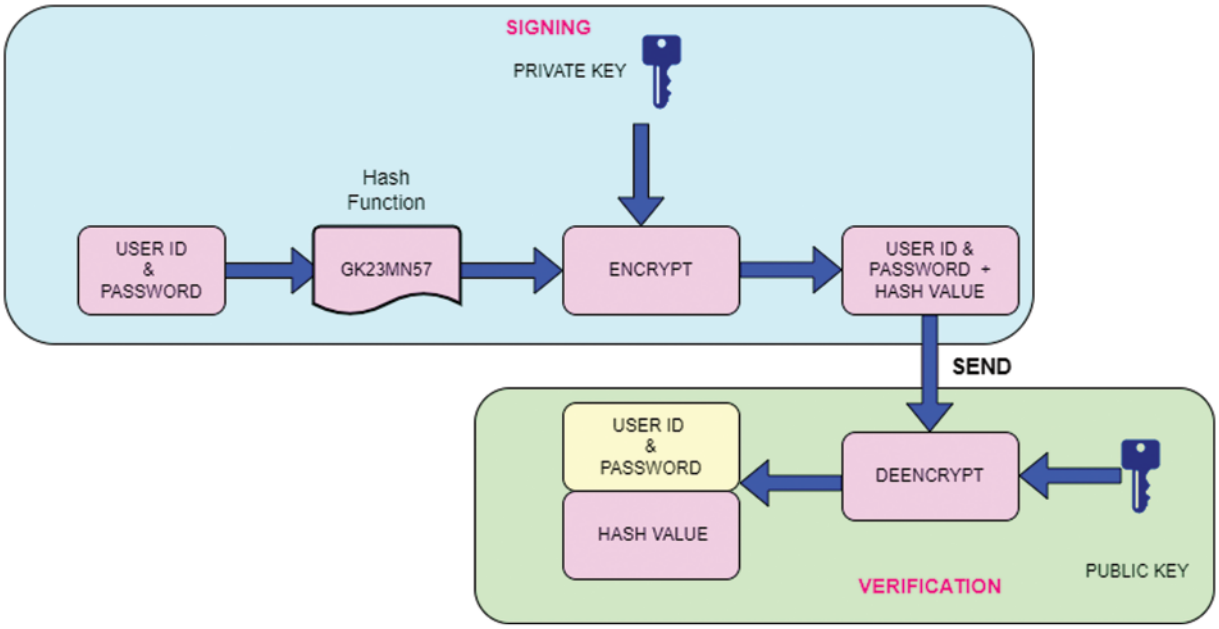

Figure 2: Workflow of the verification process

The working procedure of Fig. 2 describes below.

Step 1: The credential information of user C is passed into a hash f on $H\#$.

Step 2: Credential information with hvalue cane $H\#$ are encrypts with sender's private key.

Step 3: Decrypt the information by using the sender's public key.

Step 4: Once it decrypts the information, it is passed through the same hash function ($H\#$), to generate the original information.

In this way, it can store the credential information of the registered user in high-level security. For providing security authentication for sharing information, we used a blockchain of distributed network with all the users (nodes). Each user generates two keys; a public key used by other users to send messages among the nodes, and a private key used to encrypt the information. For the security authentication scheme, in this work, we proposed the RSA algorithm

Algorithm 1: Generate Key (Step 1)

The public key of the receiver encrypts the plain text, while t private key of the receiver decrypts the encrypted message. For the key generatio,the RSA algorithm uses two large prime numbers m, n.

1. Select m, n
2. Evaluate $l = m * n$
3. Evaluate $\phi(l) = (m-1) * (n-1)$
4. Select integer *pub* and *pub* is a public key.
5. $gcd(\phi(l), pub) = 1; 1 < pub < \phi(l)$
6. Calculate *pri* and *pri* is a private key.
7. $pri = pub^{-1} mod\ \phi(l)$
8. Public key: $pubkey = pub, l$
9. Private Key: $prikey = pri, l$

After the provider generates a pair of public keys and private keys for every user, the security is established. Fig. 3. shows that the proposed hybrid architecture of two fish with RSA.

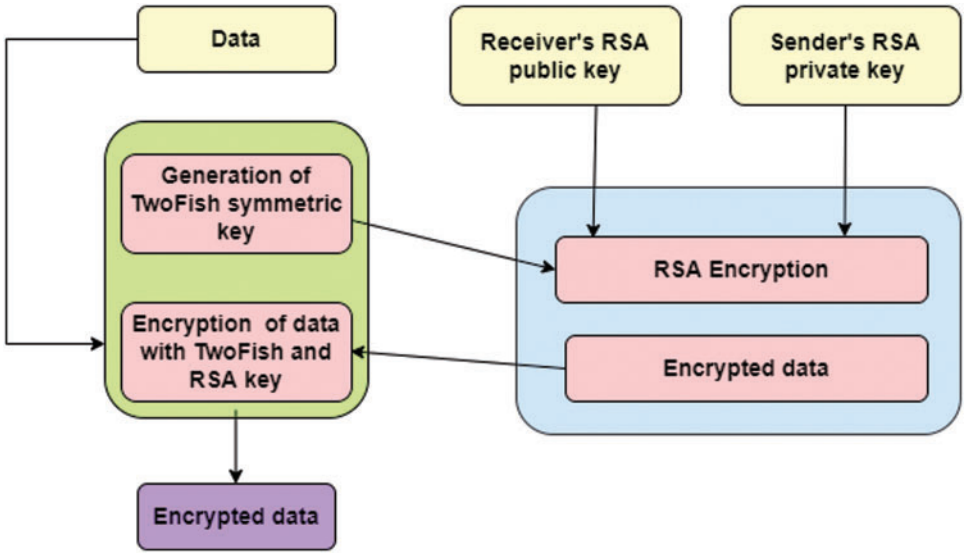

Figure 3: Hybrid architecture of two fish with RSA

To generate the encrypted file F1, user A first uses RSA with its public key. By using the second layer, user B generates the encrypted file F2. Finally, user Auploads two encrypted files: F1 and F2 into the server.

$Encryptt = encr\,(en, m_k)$

Step 3: Make *en* information to be encrypted.

Step 4: Calculate ciphertext by using following formula,

$C = P^e mod\ n, P < n$

C Ciphertextext; P is Palin text; e is an Encryption key and n is block size.

Step 5: Construct a decryption key

$P = C^d mod\ n$

User A requests the public key from the cloud service provider. The provider will return this public key to User A. User Auses the public key and User B uses a private key to generate the decryption key, and then User Auploads the newly generated decryption key into the server.

Step 6: Calculate the public key and private key *Rpubk*, *Rprik*.

Step 7: The homomorphic Paillier algorithm generates the dciphertextpher text and the public key *Rpubk* is sent to the cloud computing services.

Step 8: The public key *Rpubk* and the seconciphertexther text, this algorithm can use the decryption key and generate the firsciphertexther text of the public key *Rpubk*.

Step 9: The cloud server uses the decryption key and the ciphertext uploaded by User A. to conduct proxy decryption computing and generates new ciphertext.

Step 10: User B requests data and $decrpt \rightarrow decrypt\ (pri, b_k)$

Step 11: User B requests the cloud server to decrypt the data and the corresponding ciphertext. The cloud server sends the decrypted text to Medical Institution Band and uses RSA for decryption to get the original.

3.2 Data Storage Securely Using TF-RC-Proposed

The registered user can upload or download the information in a secure manner. For the secure storage of information encrypt the information and stored it in the cloud. For this encryption, this paper proposes two fish algorithm with a ripple consensus algorithm in the blockchain. Two fish algorithm is implemented as given below:

Algorithm 2:

Step 1: Read the input data in the block size of 128 bits and divide it into four chunks, each chunk contains 32 bits of word size.

Step 2: The single chunk input word size 32-Bit is XORed with the four key parts.

$$B_{0,i} = D \oplus K_i; i = 0\ to\ 3 \quad (1)$$

where K is a key and K_i is a subkey i = 0 to 3.

The first word is XORed with $K_{the\,0}$, second word is XORed with K_1 and so on.

Step 3: Two fish algorithm is based on the concept of the Feistel network.

Step 4: In the substitution box (S-box), the first word is divided into 4 bytes. And the second word is rotated left by 8 bits and applied to the same set of S-boxes.

Step 5: Diffusing the first and second words (32-bit word amongst 4 bytes) were applied to Maximum Distance Separable (MDS).

Step 6: After applying MDS matrix multiplication the first word is applied to a pseudo-Hadamard Transform:

mm′ = mm + nnrrrrrr 232

where m is the first word, is the second word and m' is the new first word.

Step 7: Choose the 'new' first-word m′ as input, then applied second-word n to the same transform, which can be denoted as: mm′ = mm +2nnrrrrrrrr 232.

(Continued)

Algorithm 2: Continued

Step 8: At this stage, the first two words are XOR'ed with a round key.
Step 9: The output of the new first word is XOR'ed with the third word and rotated right by a single bit which produces a new third world. Similarly applying rotation left (Single bit) to the fourth word and XORed with the second word produces a new fourth word.
Step 10: To begin with the second round, choose the first and second words of the previous round became the third and fourth words of this round. Now new first and second words are the output of previous rounds.

3.2.1 Components of Ripple Protocol

Step 11: Repeat Steps 4 to 10 until all words are XORed with another set of round keys.

Step 12: Swapping first and second words with third and fourth words effectively. The words are XOR with another set of round keys ($KK4-KK7$) producing the ciphertext.

By applying Algorithm 2, registered users' information is stored in the blockchain-based cloud storage. In this proposed work, blockchain [29,30] uses the Ripple Consensus protocol. This was used in the distributed network for solving the issues like accurate storage of information, utility, and agreement.

There are six components in the ripple protocol. They are Server, Ledger, Last Closed Ledger, Open Ledger, proposer, and Unique Node List (UNL).

1. Server–To execute the consensus process it runs ripple server software.
2. Ledger–For keeping the history of transactions, updating transactions, and successfully committing transactions Ledger is used.
3. Last Closed Ledger-Last successfully updating copy of the ledger.
4. Open Ledger–Here, transactions of information details are stored as a local copy of a node.
5. Proposer-Multiple transactions from registered users are included in the consensus process, but the only server of the UNL list would be accepted.
6. Unique Node List (UNL)-Each server has a unique node list of servers which helps in the process of consensus.

The Ripple consensus algorithm runs in all nodes in the server in a specific interval of time. All nodes in the network must contain a closed ledger. The procedure to run the Ripple consensus algorithm is given below:

Step 1: Using Algorithm 1, all new valid transactions are chosen by the servers and considered as a candidate set.

Step 2: Combining all candidate sets of the servers which belong to the UNL and start voting.

Step 3: Transactions that receive more than the minimum percentage of votes are moved to the next round remaining transactions are discarded or begin from the first round.

Step 4: The leading transactions are more than 80% which process from open to last close ledger is taken as a final collection of transactions.

By using this consensus algorithm, it needs low latency in a distributed network. This is the main advantage of using this protocol.

3.2.2 Cloud Storage

After implementing the TF-RC, storing all transactions in the blockchain based on the cloud storage system. This provides a more secure and encrypted file that is uploaded to the cloud and it would be downloaded from the cloud using decrypted format without exposing of details of the registered user. Fig. 4 shows that the architecture of the proposed work

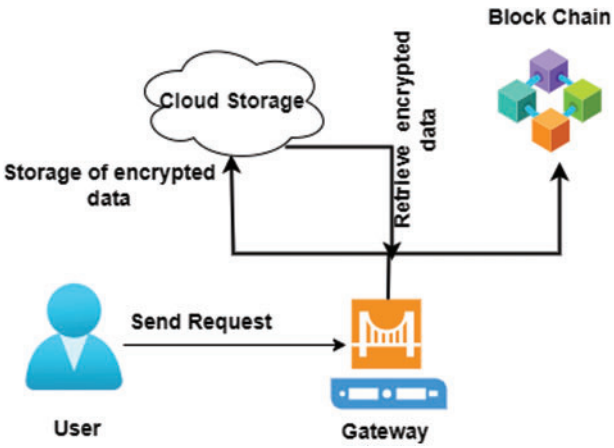

Figure 4: Architecture of proposed work

From Fig. 4, based on the request from using the encrypted file is stored in the cloud database in more secure. When it is needed it will be downloaded from the cloud decrypt for further usage. This way it can maintain the data integrity of the registered user with proper login credentials. The users can access data based on permissions set by the administrator.

3.3 Updating Authenticated Information

Registered User A will send a request to the TF-RC system for getting authentic updating information by using the following procedure:

Step 1: Registered user A receives ID and password from the certificate authority. Then maintaining the secure connection between the user and the TF-RC system is verified.

Step 2: The blockchain ripple protocol verifies and validates the registered user's information and generates the authorization with a random key number.

Step 3: This random key number along with encrypted information is distributed in the network and saved in the cloud server.

3.4 Detection of Breaches in the Distributed Network

The registered user utilizes its secret key (random key) to upload and downloads the information from the cloud storage. The offender attached the registered user's credential information and sends a request to share information. That suspicious with a fake detail are detected in the TF-RC system. This proposed work will track the malicious activity by using blockchain authenticated users.

4 Performance Analysis

In this section, performance is analyzed in the proposed TF-RC system using blockchain technology through parameters of latency, efficiency, privacy, running time, and reliability. Data is generated and stored in a secure way. In order to show the high dimensionality in security and feasibility of TF-system using blockchain technology-based cloud computing is used. This proposed work TF-RC was implemented in Java programming language. After implementing this software component overall test is executed by Apache JMeter. The main contribution of our work is to provide security in storing and sharing information. Algorithm 2 describes the formulation of the two fish encrypted concept. It interacts with a blockchain-based cloud service provider and accesses the stored information in blocks with the permissions assigned to the user. Tab. 2 shows the result obtained by using TF-RC with cloud computing.

Table 2: Results obtained by TF-RC using cloud computing

Total request	Average access time (ms)	Standard deviation (ms)
1	365.67	184.05
100	1889.45	145.21
200	3557.23	135.67
500	5728.78	145.12
1000	8367.38	124.89

A number of active user requestors between 10 and 100 users for periods of 4 min, 6 min, 10 min, 15 min, 20 min, and 50 min. It also detects all attacks based on the number of non-registered users who are trying to access the data information. The latency has been evaluated by analysing the time taken to deliver of data after a request has been sent by the users. This is shown in Tab. 3.

$$latency\ of\ service\ delivery = Completion\ time\ of\ task + Network\ propagation \tag{2}$$

Table 3: Latency per number of user's requests

No. of users	Latency (Sec)
10	165.67
20	267.78
30	361.78
40	475.65
50	580.23
60	690.98
70	765.22
80	875.67
90	986.45
100	1130.64

An important observation of Tab. 3 shows on the latency time is increases with the request of the user increases. This is due to the trade-off between securities on data over low latency. Even though the latency time increases but efficiency is maintained by two fish encryption algorithm. In an analysis of the program execution process based upon the encryption and decryption of the file with a different size, a result is generated. A comparison table of encryption and decryption using various methods is given in Tab. 4.

Table 4: Encryption and decryption execution time in seconds

File name	File size	Twofish		RS		Twofish + RSA		Proposed TF-RC with RSA	
		Encrypt	Decrypt	Encrypt	Decrypt	Encrypt	Decrypt	Encrypt	Decrypt
101.txt	100 kb	0,084	0,041	0,088	0,039	0,083	0,027	0,077	0,022
201.txt	200 kb	0,243	0,049	0,211	0,051	0,189	0,045	0,194	0,030
301.txt	300 kb	0,312	0,078	0,298	0,071	0,289	0,067	0,250	0,057
401.txt	400 kb	0,421	0,125	0,395	0,121	0,389	0,118	0,370	0,115
501.txt	500 kb	0,765	0,187	0,689	0,182	0,675	0,175	0,620	0,160

In the observation of Tab. 4 encryption and decryption time needs for our proposed work got less time and compare it with other methods. Fig. 5 shows that reliability of data storage.

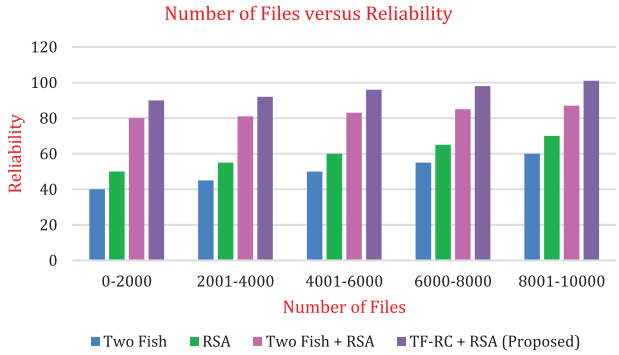

Figure 5: Reliability of files

The observation of Fig. 5 describes the reliability obtained from four different methods with a number of files in the data storage. Our proposed method TF-RC got better reliability when the number of files gets increased.

Throughput

In this parameter, it is the rate at which valid transactions of data are committed by the blockchain.

$$transaction\ per\ block = \frac{block\ size}{average\ transaction\ size} \tag{3}$$

$$fraction\ of\ block\ per\ second = \frac{1}{block\ time\ in\ seconds} \tag{4}$$

$$transaction\ per\ block = transcation\ per\ block * fraction\ of\ block\ per\ second \tag{5}$$

This throughput parameter is compared with Two Fish, RSA, Two Fish + RSA and our proposed work TF-RC with RSA. Fig. 6 shows the comparison of throughput.

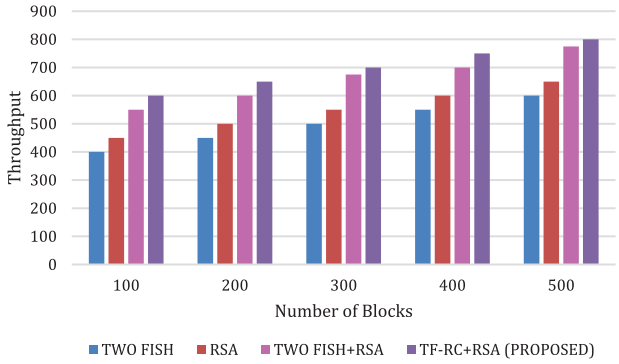

Figure 6: Throughput

In the observation of Fig. 6 shows that, our proposed work executes more blocks in a period of time.

Energy Efficiency

Authentication is needed for the accessing the data from the block chain. This average energy efficiency (bits/sec/joule) parameter checks each block with threshold value of 5 joules. Fig. 7 shows the comparison of energy efficiency parameter with TF-RC.

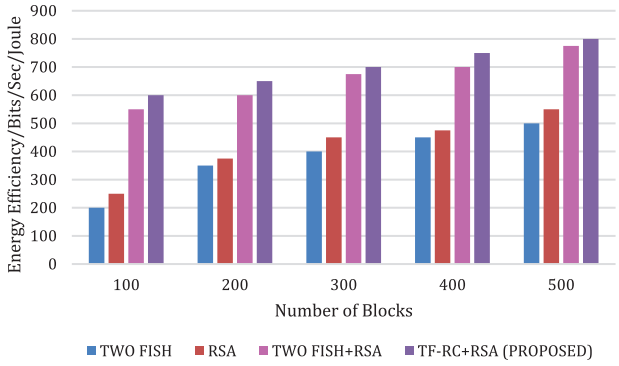

Figure 7: Energy efficiency

The proposed method TF-RC with RAS shows that the average energy efficiency has increase in the transmission of data among the chains in the block. Fig. 8 shows that running time of files.

Fig. 8 shows that the running time obtained from various methods of two fish, RSA, Two Fish with RSA and our proposed work along with its number of files in the data storage. Our proposed work TF-RC executes in a fast manner. If number of files increases, running time also increases. Fig. 9 shows that average access time for medical data in the IoMT based blockchain system.

Accessing data from the blockchain our proposed work requires minimum time. Tab. 5 shows the cost of communication and storage cost in bits of different techniques.

From the observation of Tab. 5, our proposed work TF-RC got minimum communication cost bit and storage cost bit than other techniques.

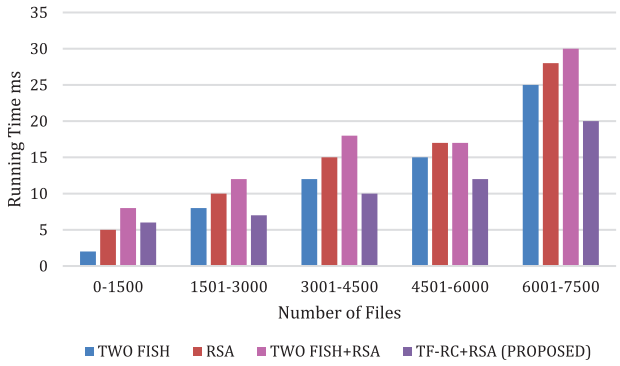

Figure 8: Volume of data (number of files) *vs*. running time

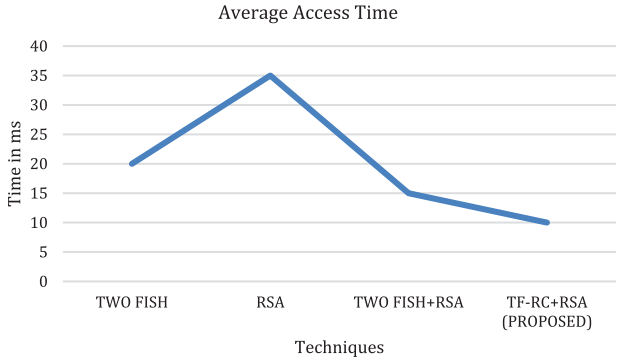

Figure 9: Average access time

Table 5: Communication cost and storage cost of different methods

Algorithm	Communication cost (bits)	Storage cost (bits)
Two fish	4360	6350
RSA	3580	2725
Two fish + RSA	2770	1580
TF-RC (Proposed)	1530	1280

5 Conclusion

This paper demonstrated the Enhancing Blockchain security using the Ripple consensus algorithm in an effective way. Data are collected and preserved in the cloud storage based on blockchain technology in a secure manner as well as detection of breaches needs more intelligent methods. Therefore, in this work, TF-RC is implemented. It consists of registration of the user, authentication, encryption of data, and secure storage of data. In the distributed network system by using our proposed work, the level of security is improved. TF-RC provides maximum benefits in the terms of privacy-preserving, security, and maintains a high dimensionality process effectively. Data integrity and reliability also improved. In the future, this work will extend up to the processing of collecting information in the blockchain-based technology to provide security for the attacks like DDoS, DoS,

and so on. Implement a novel technique for proving security without increasing the computational overheads of the model. Also, providing efficient hash algorithms to ensure the durability of the model. In the future, other consensus protocols can be included.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Velmurugadass, S. Dhanasekaran, S. S. Anand and V. Vasudevan, "Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021.

[2] W. Yang, E. Aghasian and S. Garg, "A survey on blockchain based internet service architecture: Requirements, challenges, trends, and future," *IEEE Access*, vol. 7, pp. 75845–75872, 2019.

[3] J. Yu and H. Wang, "Strong key exposure resilient auditing for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1931–1940, 2017.

[4] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[5] H. Honar Pajooh, M. Rashid, F. Alam and S. Demidenko, "Multilayer blockchain-based security architecture for the internet of things," *Sensors*, vol. 21, no. 3, pp. 772, 2021.

[6] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Software*, vol. 34, no. 6, pp. 21–27, 2017.

[7] M. Padmavathi and RM. Suresh, "Secure P2P intelligent network transaction using Litecoin," *Mobile Networks and Applications*, vol. 24, no. 2, pp. 318–326, 2018.

[8] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," *Lecture Notes in Computer Science*, vol. 8617, pp. 421–439, 2017.

[9] P. Katsiampa, "Volatility estimation for Bitcoin: A comparison of GARCH models," *Economics Letters*, vol. 158, no. 1, pp. 3–6, 2017.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* "MeDShare: Trustless medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, no. 99, pp. 14757–14767, 2017.

[11] G. Liang, S. R. Weller, F. Luo, J. Zhao and Z. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 162–173, 2019.

[12] W. Pennington and J. Evans, "Blockchain-enabled, subscriber-based capital markets index data distribution," *E-Journal of Index Investing*, vol. 7, no. 4, pp. 83–87, 2017.

[13] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proc. C'10: Proc. of the 14th Int. Conf. on Financial Cryptography and Data Security*, Tenerife, Canary Islands, pp. 136–149, 2010.

[14] X. Dai, H. Dai, C. Rong, G. Yang and F. Xiao, "Enhanced semantic aware multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Cloud Computing*, vol. 143, pp. 1, 2020.

[15] H. Wang, Q. Wang and D. He, "Blockchain-based private provable data possession," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2379–2389, 2019.

[16] S. Bamakan, A. Motavali and A. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, pp. 113385–113396, 2020.

[17] T. Frikha, H. Choura, N. Abdennour, O. Ghorbel and M. Abid, "ESP2: Embedded smart parking prototype," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 6, pp. 1569–1576, 2020.

[18] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. BenAmor *et al.,* "Implementation of blockchain consensus algorithm on embedded architecture," *Security and Communication Networks*, vol. 2021, pp. 1–11, 2021.
[19] C. Ravikumar and D. Isha Batra, "The hybrid adaptive crypto cloud framework by combining blockchain technology and botnet," *International Journal of Research Publication and Reviews*, vol. 2, no. 2, pp. 520–530, 2021.
[20] D. Pradeepa and P. Sumathi, "Adaptive secure and dynamic encrypted cloud data using elliptic curve cryptography," *International Journal of Innovative Research in Advanced Engineering*, vol. 8, no. 3, 2021.
[21] V. Gudditti and P. Venkata Krishna, "Adaptive lightweight encryption algorithm for securing multi-cloud storage," *Turkish Journal of Computer and Mathematics Education*, vol. 12, pp. 9, 2021.
[22] I. AbuElezz, A. Hassan, A. Nazeemudeen, M. Househ and A. AbdAlrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *International Journal of Medical Informatics*, vol. 142, pp. 104246, 2020.
[23] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan *et al.,* "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, no. 15, pp. 102731, 2020.
[24] L. Ismail, H. Materwala and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.
[25] S. Wang, D. Zhang and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," *IEEE Access*, vol. 7, pp. 102887–102901, 2019.
[26] J. Sun, L. Ren, S. Wang and X. Yao, "Multi keyword searchable and data verifiable attribute based encryption scheme for cloud storage," *IEEE Access*, vol. 7, pp. 66655–66667, 2019.
[27] D. Anjana and M. Ramya, "Two fish algorithm implementation for lab to provide data security with predictive analysis," *International Research Journal of Engineering and Technology*, vol. 4, no. 5, pp. 3033–3036, 2017.
[28] F. Jabeen, Z. Hamid and W. Abdul, "Enhanced architecture for privacy preserving data integration in a medical research environment," *IEEE Access*, vol. 5, pp. 13308–13326, 2017.
[29] T. R. Gadekallu, Q. V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa *et al.,* "Blockchain for edge of things: Applications opportunities and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964–988, 2021.
[30] S. Hakak, W. Z. Khan, G. A. Gilkar, B. Assiri, M. Alazab *et al.,* "Recent advances in blockchain technology: A survey on applications and challenges," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 38, no. 1, pp. 82–100, 2021.