INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS

Received: 29-03-2022

Accepted: 22-09-2022

Published: 31-10-2022

Citation: Pradeep R, Sunitha NR (2022) A Reliable Block-Chain Based Biometric Authentication Solution for Aadhar. Indian Journal of Science and Technology 15(41): 2115-2120. https://doi.org/10.17485/IJST/v15i41.658

* **Corresponding author**.

pradeepr@sit.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

A Reliable Block-Chain Based Biometric Authentication Solution for Aadhar

R Pradeep[1]*, **N R Sunitha**[2]

1 Research Scholar, Department of CSE, Siddaganga Institute of Technology, Tumakuru, 572103, Karnataka, India
2 Professor, Department of CSE, Siddaganga Institute of Technology, Tumakuru, Karnataka, 572103, India

Abstract

Objectives: To propose a reliable Block-chain based Biometric Authentication Solution (BBAS) for the Aadhar biometric authentication system. **Methods:** We have used Sokoto Coventry Fingerprint Dataset (SOCOFing) data set for biometrics. The presented model was implemented using the Ethereum network Geth (v.1.9.25) and Solidity (v.0.6.0). Python 3.8 and Web3py were used at the client side. **Findings:** From the proposed solution, it is inferred that the BBAS avoids the single point of failure problem as the biometrics are distributed throughout the block-chain. **Novelty:** This research proposes a new hybrid scheme that uses a block-chain that stores the hash value of the biometric files and a trusted third party (Aadhar) to store the biometric files, thereby avoiding storing the same bio-metric files throughout the block-chain.

Keywords: Biometric; Blockchain; Aadhar; Security; Authentication

1 Introduction

Major security flaws in biometric authentication systems include the possibility of biometric information leakage, the unreliability of authentication modules, and the lack of openness in the handling of biometric information. Because each person's biometrics are distinct and must be maintained securely, and replication of a biometric template is difficult, its application systems are more secure than conventional techniques like passwords[1]. Since biometrics are immutable, consecutive security hazards may result from a biometric data breach[2]. The majority of the time, a central agent, like AADHAR, is in charge of managing biometric data, which ensures the security and dependability of authentication systems[2]. Current research has mostly focused on the safe administration of biometric templates in order to reduce security vulnerabilities[3]. Instead of dealing with the actual biometric data, predefined characteristics are taken from the data, mixed with hash values, and then saved in the form of a template. Once the template is exposed, reverse engineering may be used to approximate the original data by the attackers. Also, if the server goes down then it leads to reliability problem of the system[4]. All these mentioned problems will be fixed using our proposed Block-chain based Biometric Authentication Solution.

Block-chain is a fast-expanding technology that combines distributed immutable ledgers, consensus algorithms, and smart contracts to produce an incorruptible digital ledger capable of recording and validating any form of transaction. Bitcoin, for example, makes use of block-chain technology to maintain a record of bitcoin transactions. Similarly, our suggested approach employs block-chain technology for biometric-based user authentication. The client-server approach for authentication security systems creates a single point of failure problem when the server goes down or the client is not able to connect to the remote server. Incorporating block chain technology into the authentication system eliminates the single-point-failure problem. The system suggested in this research illustrates both the feasibility and the robustness of the method against cyber assaults. Block-chain technology has been tested and proven in a variety of fields, including cryptocurrencies, healthcare, supply chains, and the Internet of Things. Public and permissioned block-chain designs are the most common[(5)]. Furthermore, for greater cost efficiency and speed, most permissioned block-chains employ Byzantine Fault Tolerance-based (BFT) consensus methods[(6)]. Even if some participants are hacked or misbehaving, BFT is a consensus system that assures consistency and low latency.[(7)]. In this work, the authors used block-chain to secure firmware upgrades. Using public block-chains, the authors of[(5)] developed solutions for generic IoT devices and showed that the block-chains may be used to secure any type of transaction record[(7)]. They've been investigated in a variety of fields, including firmware upgrades.[(8)]. In this study, a block chain-based biometric authentication scheme for supply chain management is proposed, in which all employees are authenticated using a mobile phone finger print sensor. However, this scheme fails to ensure that original data stored on the blockchain accurately reflects reality, particularly information about people involved in cargo handling.[(9)] This study demonstrates all of the potential drawbacks of block chain technology. One of the most significant issues is storage capacity on each block chain node. The primary limitation of data storage on a blockchain is the quantity of data that can be stored. This is either because the protocol limits the amount or because the transaction costs would be too high. Data storage on the block chain is prohibitively costly due to the fact that the quantity of data you store must be stored by every complete node on earth. Everyone who gets the blockchain is also getting your information. This is why storing even a few kilobytes may be prohibitively expensive. When storing data on the blockchain, we typically pay a basic transaction fee plus a fee for each byte we want to store. If smart contracts are used, we additionally pay for the smart contract's execution time. In this work we have used the Sokoto Coventry fingerprint dataset[(10)] for the experiment, and it is a biometric fingerprint repository created for scholarly study. 6,000 fingerprint scans from 600 African people make up SOCOFing. Unique characteristics of SOCOFing include labels for the gender, names of the hands and fingers, and variants that have undergone three various degrees of artificial modification, including obliteration, central rotation, and z-cut. The data collection is readily accessible for academic study.

2 Methodology

In this part, we provide the findings of our assessment and prototype implementation. The Ethereum network Geth (v.1.9.25) and Solidity (v.0.6.0) were used to create our prototype, while Python 3.8 and Web3py were used for the client.

We analytically assessed BBAS performance in real-world circumstances to verify its dependability. Assume that there are 3n clients in BBAS (n = 1, 2, 3, etc.), and each client is responsible for managing n copies of each fragment. The functioning of BBAS may thus be ensured as long as less than n clients are disabled. However, its authentication would not be possible if more than 3n-2 clients were deactivated.

$$P=\frac{f}{g},\left(f=\sum_{(i,j,k)\in X}\frac{(3n-x)!}{i!j!k!},g=\frac{(3n)!}{n!n!n!}\right) \tag{1}$$

$$\mathrm{X}=\{(\mathrm{a},\mathrm{b},\mathrm{c})\mid \mathrm{a}>0,\ \mathrm{b}>0,\mathrm{c}>0\wedge \mathrm{a}+\mathrm{b}+\mathrm{c}=3\mathrm{n}-\mathrm{k}\} \tag{2}$$

Let x represent the number of disabled clients (n 1 x 3n2) and P represent the probability of a successful authentication (see Eq. (1)): Instances in which certain clients are disabled but still have several pieces of each template accessible for completing authentication are represented by the numbers I, j, and k. Instances in which n copies of each fragment are kept across 3n clients are represented by the number g.

Figure 3 shows the outcome of P with 3n (n = 2,3,4). If two of the five clients in a BBAS are deactivated, then there is a 40% chance that authentication will proceed correctly. If two of the eight clients in BBAS are deactivated, the regular authentication process may be ensured. With a chance of 32%, authentication is still possible even if three of them are disabled. Since BBAS ensures more stable authentication operation, it outperforms conventional authentication systems, which cannot guarantee authentication operation if their central server is offline.

In order to evaluate the effectiveness of BBAS, we built a typical authentication system with one server and one client. The execution times of the server-client system and the BBAS prototype were compared while running on Virtual Box-capable VMs (Ubuntu LTS 22.04, 8GB RAM, 100GB HDD storage). Three clients, each of which is in charge of a different split template. A template's size was set to 2KB, which is considered to be a standard template size. Between extracting the template and authenticating, we timed the BBAS authentication process. Over BBAS's five repetitions, the LookUp smart contract's conclusion was obtained on average in 352 milliseconds, whereas split template fragments from other clients were obtained in 167 milliseconds (519 ms in total). It took 201 milliseconds to complete the authentication for the server-client system, in which a client requests and receives a template from a server. It is clear from the little time difference between the systems that BBAS ensures the reliability of its authentication process while incurring no performance overhead. The fact that recording an authentication action took a considerably longer amount of time (1,906 ms), although having no bearing on the authentication process, has no impact on BBAS's performance in terms of authentication.

To perform biometric based authentication, the biometrics of each and every individual have to be stored in a secure database such as Aadhar, which was created by the Unique Identification Authority of India (UIDAI). Every subject who is enrolled in the biometric system will be issued a 12-digit Unique Identification (UID) number. As the Aadhar contains 1.2 billion Indian residents, by the end of 2014, this will create a database of about 15 petabytes in size. Storing this huge data on the block chain is the biggest challenge and comes with significant cost and creates redundancy. To overcome this issue, we have proposed a new hybrid approach that includes both the block chain and a central Aadhar biometrics server.

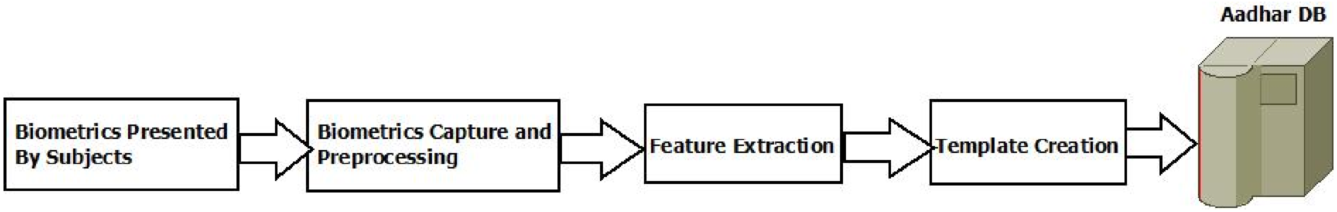

Aadhar DB
Biometrics Presented By Subjects
Biometrics Capture and Preprocessing
Feature Extraction
Template Creation

Fig 1. Biometric Enrollment without Block Chain

Figure 1 shows the biometricenrollment process, which mainly includes 4 steps, where in the first step, the subject is going to present his biometrics, such as finger prints, iris or face, on biometric capture devices (sensors). In the second step, the biometrics were captured and preprocessed using the biometric enrollment hardware and software SDKs. The quality checks were done at this stage. In the third step, the features (areas of interest) are extracted from the captured biometric images and, finally, a biometric template is created for the enrollment and it will be stored on the Aadhar DB. Aadhar is a client-server-based architecture for biometric enrollment and authentication, which may cause a single point of failure problem.

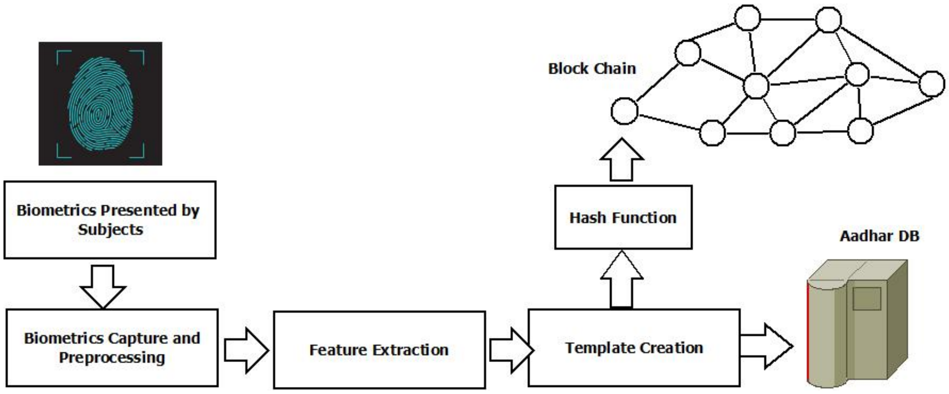
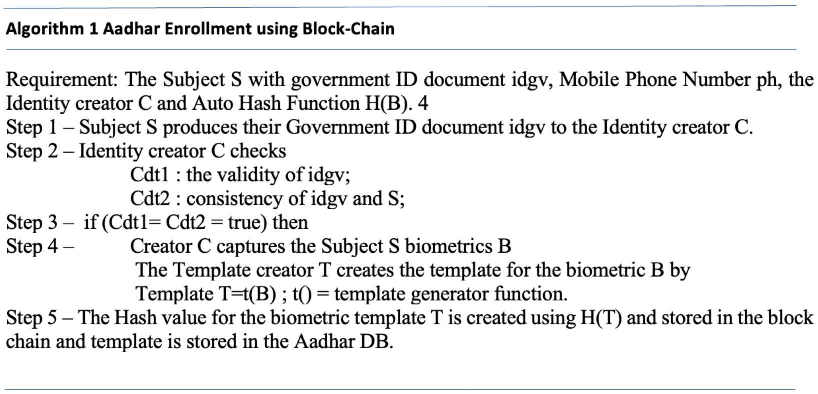

Block Chain
Hash Function
Aadhar DB
Biometrics Presented by Subjects
Biometrics Capture and Preprocessing
Feature Extraction
Template Creation

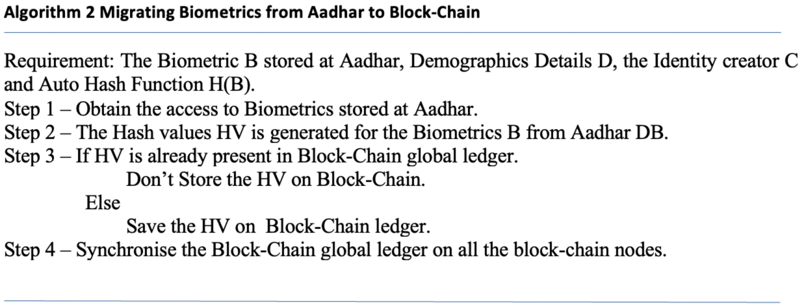
Fig 2. Proposed Solution for Biometric Enrollment

In the proposed solution, a hybrid approach is used in which instead of storing the biometric template files in each and every node of the block chain, a one-way hash function is used in which for every biometric template, a unique hash value is generated and these values are stored in the block chain nodes. The biometrics enrollment along with Aadhar and Blockchain is explained in Algorithm 1. From the algorithm, it is clear that the biometric templates will be stored on Aadhar DB and a hash value generated for the template will be stored on block chain nodes. Algorithm 2 shows the migrating of the already enrolled biometrics from Aadhar to the block chain.



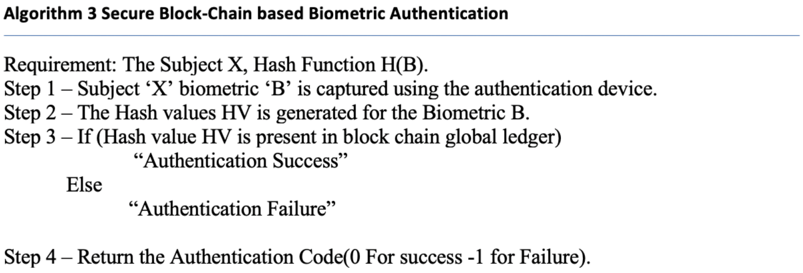
Algorithm 1 Aadhar Enrollment using Block-Chain

```
Requirement: The Subject S with government ID document idgv, Mobile Phone Number ph, the
Identity creator C and Auto Hash Function H(B). 4
Step 1 – Subject S produces their Government ID document idgv to the Identity creator C.
Step 2 – Identity creator C checks
                 Cdt1 : the validity of idgv;
                 Cdt2 : consistency of idgv and S;
Step 3 – if (Cdt1= Cdt2 = true) then
Step 4 –         Creator C captures the Subject S biometrics B
                  The Template creator T creates the template for the biometric B by
                  Template T=t(B) ; t() = template generator function.
Step 5 – The Hash value for the biometric template T is created using H(T) and stored in the block
chain and template is stored in the Aadhar DB.
```



Algorithm 2 Migrating Biometrics from Aadhar to Block-Chain

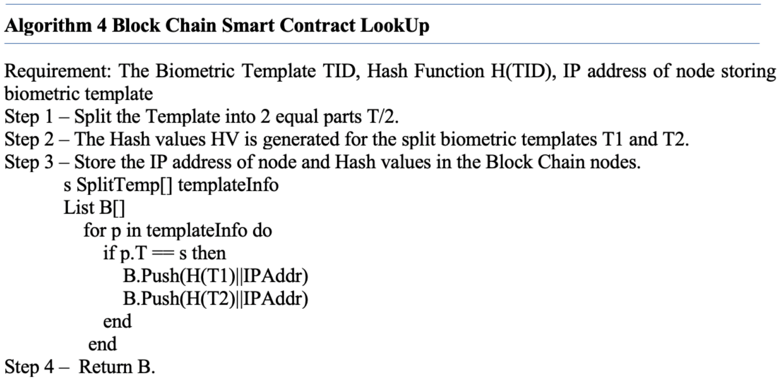
```
Requirement: The Biometric B stored at Aadhar, Demographics Details D, the Identity creator C
and Auto Hash Function H(B).
Step 1 – Obtain the access to Biometrics stored at Aadhar.
Step 2 – The Hash values HV is generated for the Biometrics B from Aadhar DB.
Step 3 – If HV is already present in Block-Chain global ledger.
                 Don't Store the HV on Block-Chain.
           Else
                 Save the HV on  Block-Chain ledger.
Step 4 – Synchronise the Block-Chain global ledger on all the block-chain nodes.
```



Algorithm 3 Secure Block-Chain based Biometric Authentication

```
Requirement: The Subject X, Hash Function H(B).
Step 1 – Subject 'X' biometric 'B' is captured using the authentication device.
Step 2 – The Hash values HV is generated for the Biometric B.
Step 3 – If (Hash value HV is present in block chain global ledger)
                 "Authentication Success"
         Else
                 "Authentication Failure"

Step 4 – Return the Authentication Code(0 For success -1 for Failure).
```



Algorithm 4 Block Chain Smart Contract LookUp

```
Requirement: The Biometric Template TID, Hash Function H(TID), IP address of node storing
biometric template
Step 1 – Split the Template into 2 equal parts T/2.
Step 2 – The Hash values HV is generated for the split biometric templates T1 and T2.
Step 3 – Store the IP address of node and Hash values in the Block Chain nodes.
         s SplitTemp[] templateInfo
         List B[]
            for p in templateInfo do
               if p.T == s then
                  B.Push(H(T1)||IPAddr)
                  B.Push(H(T2)||IPAddr)
               end
            end
Step 4 – Return B.
```

In the proposed technique the biometric is split into 2 equal parts and they are managed by different clients, the hash values for the dual split templates were generated and stored in the block chain and this technique avoids leaking of complete biometric in case of attacks . Hashing algorithms can be used for a variety of tasks such as saving passwords, computer vision, and data storage in databases, among others. SHA (Secured Hashing Algorithm) is one of several hashing algorithms that are available, and is chosen based on the speed, optimization, as well as security of the cryptographic algorithm being used. SHA produces

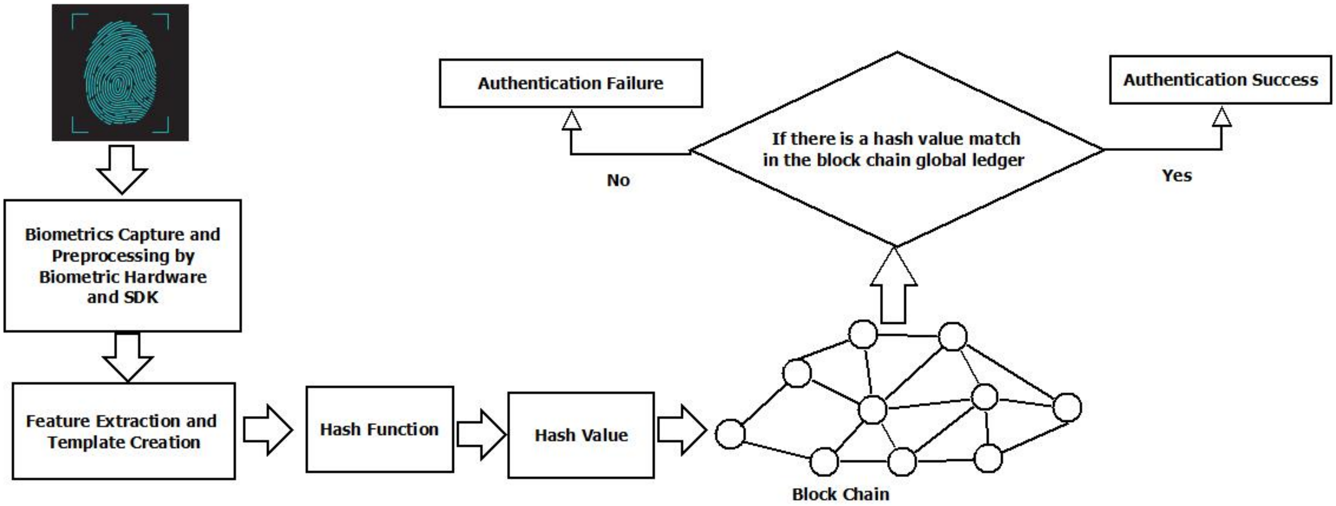

Biometrics Capture and Preprocessing by Biometric Hardware and SDK
Feature Extraction and Template Creation
Hash Function
Hash Value
Block Chain
If there is a hash value match in the block chain global ledger
No
Yes
Authentication Failure
Authentication Success

Fig 3. Secure Block-chain Based Biometric Authentication

irreversible and unique hashes and is one of the fastest hashing algorithms available. There are two methods for hashing: SHA-1 and SHA-2, which differ in terms of construction and bit length. There are many possible hashes in SHA-2, including SHA-224, SHA-384, and SHA-512, with the 256 bit hash being the most used. The secure block chain based authentication scheme is explained in Algorithm 3, in which when a subject's biometric such as finger print is captured by an authentication biometric device, a hash value is generated for that particular biometric template and checked against the block chain global ledger entry. If there is a successful match, then an authentication success code of 0 is returned to the biometric client. If there is no match between the hash value and the block chain global ledger entry, then an authentication failure -1 value is returned to the biometric client. Algorithm 4 shows the block chain smart contract look up at block chain nodes for storing the hash values for the split biometric templates.

3 Results and Discussion

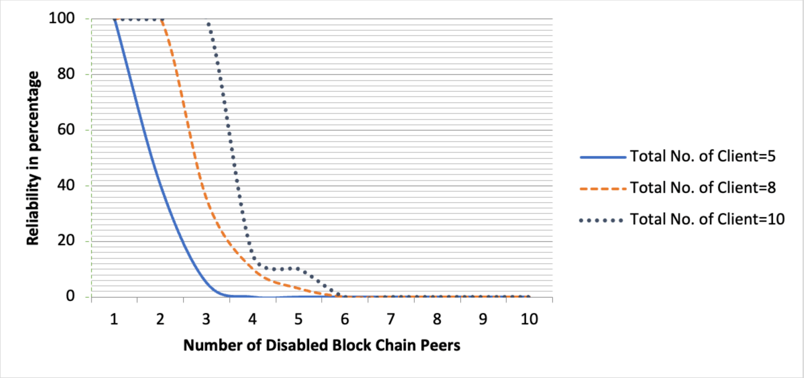


Fig 4. BBAS's reliability on different num. of disabled clients

The blockchain-based distributed and decentralised biometric authentication system known as BBAS was introduced in this study. The blockchain-based biometric authentication system (BBAS) increases the security and reliability of existing biometric identification systems by breaking a biometric template into parts and managing them in this way. In particular, BBAS (1) enhances biometric data security via distributed blockchain administration, (2) enhances authentication operation reliability through decentralised blockchain authentication, and (3) ensures biometric data flow transparency through blockchain-based audit mechanism. The split template storage and authentication client for BBAS on the Ethereum blockchain was successfully created. We can confidently claim that BBAS offers reliable authentication with very low performance overhead based on the evaluation's results.

The biometric DB such as Aadhar is very big and its size is around 15 petabytes because it stores the physical biometric templates of every single subject. For each single subject, 10 finger prints, 2 iris prints, and one face template have to be stored on the Aadhar DB, which requires big data centers. The existing block chain based biometric security systems are suitable for small-sized DB users such as office employees, college students, etc., and the existing techniques fail to store large data such as Aadhar in their block chain nodes, and it comes with significant cost and effort. Storing the Aadhar biometrics on block chain peers creates redundancy. In the proposed solution, only the hash values of the biometric templates are stored on block chain nodes. This solves all of these problems.

Table 1. Differences in authentication operation time

Authentication Type	BBAS	Client-Server
Time taken to run contract	352 ms	-
Time taken to request biometric template	167 ms	-
Total time taken for authentication	519 ms	201 ms

4 Conclusion

Block-chain based Biometric Authentication Solution BBAS solves the single point of failure problem with a negligible drop in performance/speed of authentication as compared to client-server model of authentication. The proposed BBAS solves the reliability problem by incorporating block-chain based distributed authentication scheme. By using optimization approaches for the template segmentation process and inter-node communication the performance can be further increased.

References

1) Zhu X, Cao C. Secure Online Examination with Biometric Authentication and Blockchain-Based Framework. *Mathematical Problems in Engineering*. 2021;2021:1–12. Available from: https://doi.org/10.1155/2021/5058780.
2) Gracia SJB, Raghav D, Santhoshkumar R, Velprakash B. Blockchain based aadhaar. *2019 3rd international conference on computing and communications technologies (ICCCT)*. 2019;p. 173–177. Available from: https://www.irjet.net/archives/V7/i3/IRJET-V7I3254.pdf.
3) Acquah MA, Chen N, Pan JS, Yang HM, Yan B. Securing Fingerprint Template Using Blockchain and Distributed Storage System. *Symmetry*. 2020;12(6):951–951. Available from: https://doi.org/10.3390/sym12060951.
4) Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Gener Comput Syst*. 2020;107:841–853. Available from: https://doi.org/10.48550/arXiv.1802.06993.
5) Delgado-Mohatar O, Fierrez J, Tolosana R, Vera-Rodriguez R. Blockchain and biometrics: A first look into opportunities and challenges. In: International Congress on Blockchain and Applications. Springer. 2019;p. 169–177. Available from: https://doi.org/10.48550/arXiv.1903.05496.
6) Sarier ND. Efficient biometric-based identity management on the Blockchain for smart industrial applications. *Pervasive and Mobile Computing*. 2021;71:101322. Available from: https://doi.org/10.3390/s22103956.
7) Xiang X, Wang M, Fan W. A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems. *IEEE Access*. 2020;8:171771–171783. Available from: https://doi.org/10.1109/ACCESS.2020.3022429.
8) Hassen OA, Abdulhussein AA, Darwish SM, Othman ZA, Tiun SA, Lotfy YA. Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network. *Symmetry*. 2020;12(10):1699–1699. Available from: https://doi.org/10.3390/sym12101699.
9) Páez R, Pérez M, Ramírez G, Montes J, Bouvarel L. An Architecture for Biometric Electronic Identification Document System Based on Blockchain †. *Future Internet*. 2020;12(1):10. Available from: https://doi.org/10.3390/fi12010010.
10) Shehu YI, Ruiz-Garcia A, Palade V, James A. Sokoto coventry fingerprint dataset. *arXiv preprint* . 2018;1807:10609. Available from: https://doi.org/10.48550/arXiv.1807.10609.