SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
On-line first, 1-17

DOI: https://doi.org/10.2298/SJEE240805002R

Original scientific paper

An Optimised Sidechain Based Biometric Attendance Solution

Pradeep Rajanna[1], Nagarajaiah Renukamba Sunitha[2], Hanumanthaiah Ranjini[3], Halappa Kavitha[4]

Abstract: A Biometric Authentication System (BAS) is the best choice when there is a need for end-users to have a higher level of security and reliability. However, capturing and verifying user biometrics requires dedicated biometric hardware and software systems with complex mechanisms at the back end. Most of the biometric systems are client-server architecture based, which has got the single point of failure, dependability and reliability problems. Capturing, storing and verifying biometric templates must be highly secure and reliable. When a single chain based blockchain system is used at the backend, the computational resources and verification time increase significantly due to its large block chain size. This results in more delays, inefficiencies, and requires transaction gas costs, this shows the need for block chain optimising solutions. For block chain biometric based access control systems, speed, performance, accuracy, and security are the primary requirements. In this work, we present a Side Chain based Blockchain Transaction Optimisation Solution (SBTOS) for a BAS, which is a state-of-the-art mechanism which combines the strength of blockchain and biometric technology with optimised performance for the access control systems. SBTOS mainly focuses on optimising the blockchain when used at the back end, particularly when the database size is huge.

Keywords: Block-Chain, Biometrics, Authentication, Optimisation, Side Chain.

[1]Department of Computer Science and Engineering (Cyber Security), Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumkur, Karnataka, 572105, India, pradeepr@ssit.edu.in, https://orcid.org/0000-0003-4990-1689

[2]Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, 572103, India, nrsunitha@sit.ac.in, https://orcid.org/0000-0003-4990-1689

[3]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, 572105, India, ranjinih@ssit.edu.in https://orcid.org/0009-0001-7473-351X

[4]Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru, 572103, India, hkavitha@sit.ac.in, https://orcid.org/0000-0002-5677-2953

Colour versions of the one or more of the figures in this paper are available online at https://sjee.ftn.kg.ac.rs

1 Introduction

Biometric authentication protocols [1] are a specific type of security protocol that employs a person's unique physical or behavioral traits to verify their identity. This may include biometrics [2] such as face, iris, voice, vein pattern and even a person's gait. Biometric verification protocols must be highly secure when communicating biometric data over an insecure network, as each individual's biometrics are highly confidential data that should be more difficult to replicate or forge than conventional authentication methods such as passwords or security tokens [3]. The primary benefit of the biometric security protocols is the biometrics cannot be shared to anyone just like passwords. In addition to providing a more convenient user experience, they eliminate the need for individuals to remember or carry additional credentials. There are several forms of biometric authentication protocols used worldwide, each with its own advantages and disadvantages. Depending on parameters such as precision, speed, and cost, some protocols may be better adapted for certain applications than others. Biometric authentication protocols are not ideally secure, despite their benefits. There are concerns regarding privacy and the potential for misuse or exploitation of biometric data [4], for instance. In addition, some biometric features may be more susceptible to impersonation [5] or hijacking than others. Most BAS, such as AADHAR [6] and MOSIP [7], are based on a client-server model in which the biometrics of the users are stored in centralised data centres, the client-server model creates a single point of failure problem. If the central server is down, the entire biometric verification system fails, causing a problem with the system's reliability and availability. The blockchain technology solves the single-point of failure problem and further increases the biometric back-end security. Blockchain technology [8] is a decentralised and secure digital asset recording, storage, and transmission system. It has the potential to revolutionise how transactions are conducted, but as the number of blockchain transactions increases, so does the need for optimisation. Block-chain transaction optimisation is the process of enhancing the speed, efficiency, and security of blockchain transactions through the application of a variety of techniques and technologies. The need to strike a compromise between efficiency and security is one of the primary obstacles to optimising blockchain transactions [9]. Transactions must be processed promptly to prevent delays and maintain the system's efficacy, but they must also be protected against fraud and malware. To accomplish this equilibrium, researchers have proposed a number of optimisation techniques, including increasing the block size [10], employing side chain transactions [11], and utilising multilayered networks [12]. The increased block size method is a simple and effective way to optimise blockchain transactions. By increasing the size of the blocks, more transactions can be processed at once, which can significantly increase the speed of the system. However, increasing the block size also increases the risk of centralisation, as larger blocks are more difficult to

verify and validate. Side chain transactions are the best optimisation technique that can improve the speed and efficiency of blockchain transactions. By conducting certain transactions off the blockchain, such as through payment channels, users can avoid the time and costs associated with processing transactions on the main chain. This technique has been successfully implemented in cryptocurrencies such as Bitcoin [13] and Ethereum [14]. Multi-layered networks are another approach to optimising blockchain transactions. By using multiple layers of blockchain, such as public and private blockchains [15], transactions can be processed more efficiently while maintaining the security and reliability of the system. This approach is especially useful for businesses and organisations that require high levels of security and confidentiality.

The article [16] talks about the problems with centralised storage of biometric data templates and suggests a new way to protect fingerprint templates [17] using symmetric encryption [18], peer-to-peer networking, and decentralised storage. The proposed system encrypts the fingerprint template using the Advanced Encryption Standard algorithm and saves it on the Inter-Planetary File System (IPFS), while maintaining its hash on a decentralised blockchain [19]. In addition to ensuring data integrity and preventing identity theft, the use of template hashing makes the system efficient and cost-effective. The outcomes of the experiments demonstrate how well the suggested technique secures fingerprint templates [20].

In the article [19], the authors look at the security problems with centralised authentication methods and propose a blockchain-based framework for safe and private biometric authentication. Instead of keeping biometric information on a central server, the suggested approach decentralizes and manages it using Decentralised Identifiers (DIDs) and DID papers. With total control over their biometric identity information, anonymous transactions, and the ability to be forgotten, users are now able to have self-sovereign identities and revocable pseudo-biometric identities. By applying one-way transformations to the original biometric data, the pseudo-biometric strengthens security and makes the data safe to onboard. The effectiveness of the suggested system is examined under different operating conditions.

Article [21] discusses the security issues with centralised authentication schemes and proposes a blockchain-based framework for secure and privacy-preserving biometric authentication. The proposed system uses Decentralised Identifiers (DIDs) and DID documents to decentralise and manage biometric data instead of storing it in a centralised database. This allows users to have self-sovereign and revocable pseudo-biometric identities that provide complete control over their biometric identity information, anonymous transactions, and the right to be forgotten. The pseudo-biometric adds extra protection by applying

one-way transforms to the original biometric data, making it safe to onboard. The proposed system's performance is analysed under various operating scenarios.

With an emphasis on the storage and safety of biometric template data, the authors in [22] examine the benefits and drawbacks of combining blockchain technology with biometrics. The authors talk about the real-world trade-offs that come with this integration, such as latency, processing speed, financial cost, and biometric accuracy. By altering the complexity of cutting-edge face and handwritten signature biometric systems, they experimentally assess the cost-performance of a smart contract for biometric template storage on Ethereum [23]. The research demonstrates that simple data storage strategies in blockchains may be prohibitive for storing biometric template data [24], but a blockchain approach based on Merkle trees may achieve a favourable cost-performance trade-off [25].

The use of biometric templates to store sensitive data can be secured and managed using blockchain technology, although there are certain limitations, as shown in the article [26]. It is important to find a solution for the problem of storing and protecting biometric templates. The combination of blockchain technology with biometrics includes trade-offs in terms of latency, processing speed, financial cost, and biometric accuracy. By constructing a smart contract on the Ethereum blockchain, these tradeoffs were empirically evaluated. The authors provide the source code for this implementation on GitHub for research purposes.

The article [27] examine the applicability of blockchain technology to biometrics and how the two technologies can mutually benefit one another. The implementation of blockchain technology has significantly enhanced the efficiency, affordability, and security of business operations. The study offers a comprehensive examination of blockchain technology and biometrics, with a particular emphasis on the opportunities and challenges that arise when the two are combined. The research is focused on the utilisation of blockchain technology to secure biometric templates. The research makes two significant contributions: it offers a comprehensive examination of both technologies and explores the viability of utilising blockchain technology to safeguard biometric templates.

The article [28] examines the application of blockchain technology in supply chain finance (SCF) and the compromises between security, expense, and efficacy. The implementation of blockchain technology in an inappropriate manner may lead to uneconomic outcomes or hazards for financial institution systems that are based on SCF. This paper suggests an optimisation strategy for the selection of the most effective blockchain design schemes for the SCF system, taking into account security, cost, and efficacy, using a nonlinear integer programming model. The authors have employed an algorithm that is based on ant colonies to address the optimisation problem. The optimisation model's efficacy and viability are verified by the application case analysis.

The Internet of Things (IoT) blockchain storage issue is addressed by the authors in Article [29] by suggesting Multi-Level Distributed Caching (MLDC). The decentralisation of the decrease in data duplication by MLDC is based on data access patterns. Each node is given a SC with a unique Access Frequency (AF) threshold depending on node availability as part of the implementation of a hierarchical storage class (SC). Nodes in a SC discard unavailable data from local storage based on a time threshold defined by the SC's AF threshold, thereby preserving the consistency of all block hashes. MLDC reduces network overhead in addition to reducing storage and query costs. Additionally, the security and efficacy of MLDC are evaluated for both uniform and exponentially decaying access patterns. In comparison to conventional blockchain systems, MLDC can reduce overall storage costs by 83% while maintaining data availability and blockchain integrity with only a slight increase in network overhead, as indicated by the studies.

Current systems utilising blockchain technology to enhance the KYC process are primarily conceptual and difficult to implement due to shared attributes, as discussed in Article [30]. This paper proposes and implements a blockchain-based system that reduces and distributes the cost of the KYC procedure among financial institutions (FIs) operating with a particular customer. The system provides for the dynamic updating and distribution of consumer information among participating financial institutions. Additionally, it addresses some obstacles to adoption by FIs. The outcome is a stand-alone solution that reduces the cost of the KYC process without the need for a central repository of customer data, where FIs share the initial and ongoing costs of KYC while maintaining accurate customer information.

The article [31] discusses how challenging it is to develop quality-critical decentralised applications (QCDApps) due to high performance and service quality requirements, heterogeneous infrastructures, and the need for trustworthy collaborations. Current blockchain technologies have inefficient peer-to-peer consensus collaboration, which impacts system performance. Despite significant advancements in software-defined storage, networking, and infrastructure in the cloud, QCDApps fail to effectively leverage the programmability of infrastructure, including new hardware accelerators, due to inadequate architecture and programming models.

The reviewed articles propose various methods to enhance the security and efficacy of biometric-based authentication systems and investigate the integration of blockchain technology to improve security and privacy. The techniques proposed range from using chaotic maps and cipher block chaining for image encryption [32] to utilising blockchain-based protocols for user authentication and decentralised biometric data management. When integrating blockchain and biometric technologies, the articles also emphasis the tradeoffs between security,

cost, and efficiency. Overall, biometric verification protocols have the potential to significantly enhance security and convenience in a wide range of applications, from mobile devices and financial transactions to physical access control and border security. The client-server-based model for biometric systems can cause a single point of failure, but it can be overcome using blockchain technology. As the demand for blockchain technology continues to increase, optimising transactions will be crucial to ensuring the system's scalability, security, and efficiency. Blockchain technology can reach its maximum potential as a decentralised and secure system for conducting transactions by implementing various optimisation techniques, such as side chains. Current research studies demonstrate the need for blockchain transaction optimisation techniques to enhance the efficacy and availability of the BAS using a decentralised blockchain system.

2 Side chain Based Biometrics Authentication Transactions Optimisation Solution

According to the literature, most of the existing blockchain based BAS uses a single blockchain network to store biometric templates locally and with a small chain size. The problem with single blockchain systems is that as the number of enrollments increases, the size of the blockchain network also increases. Transactions on longer blockchains will be very slow and consume more transaction gas cost. For BAS, reliability and availability are critically important. We propose and analyse the side chain based blockchain transaction optimisation solution SBTOS for fingerprint biometrics. The proposed side chain biometric authentication blockchain system combines the advantages of blockchain technology with biometric authentication to provide a safe, efficient, and scalable solution.

Sidechains are separate blockchains that communicate with the main blockchain to provide scalability and more specialised features. Let BT stand for the Biometric Template in the suggested approach. Main Blockchain (MBC) is the main blockchain that is utilised for general coordination and integrity. Sidechain (SC) An additional blockchain for certain purposes, including the storage of biometric information, A cryptographic technique called the hash function (H) converts data into a fixed-length string. Public Key Infrastructure (PKI): For safe encryption and key management, The Indexing Function (I) is a retrieval function that facilitates searchable index creation. The biometric data storage on side chain involves the below steps.

1. Template generation: For the biometric data BDi, the biometric template is generated using $BT_i=TG(BD_i)$.
2. Template Hashing and Encryption:

h_i *(hash of the biometric template* = $H(BT_i)$ and encrypt the biometric template BT_i using the public key PK_i *using* $E(BT_i,PK_i)$.

3. Store the encrypted biometric template BT_i on SC and Store h_i in Main Block Chain (MBC) for integrity verification. The storage function S can be defined as: $S(BT_i) = (SC(E(BT_i,PK_i)), MBC(h_i))$.
4. Indexing for search on sidechain:

   Create index values from biometric templates for efficient search $I(BT_i) = \{index\_values\}$ and store $I(BT_i)$ on SC. Let (h_j) be hash value set in MBC, the retrieval function R is defined as: $R(h_q) = \{BT_i \mid H(BT_i) = h_q\}$. Finally Decrypt and compare templates using indexing function I: If $I(BT_q) \approx I(BT_j)$, then fetch $E(BT_j, PK_j)$ from SC.

The proposed side chain based blockchain transaction optimisation architecture is shown in Figs. 1 and 2.

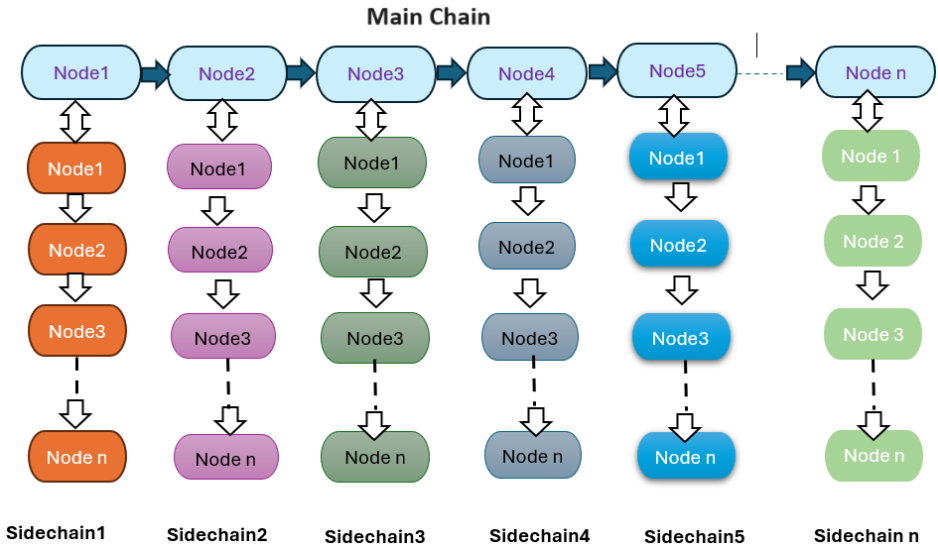

Fig.1 – *Sidechain setup for Biometric Authentication.*

The architecture is divided into two parts. 1. Enrollment; 2. Authentication. Fig. 3 shows the steps involved in the biometric enrollment part. The enrollment phase involves: 1. Capturing users biometrics using a Level-0 or Level-1 device; 2. Generating a unique identifier for the biometric and demographic data, denoted as a UID. Let's assume the biometric data is represented as a vector, denoted as $\boldsymbol{B} = [b_1, b_2, \ldots, b_n]$, where each element represents a specific characteristic or measurement of the biometric data. Once the user's biometric and demographic template is created, 3. The biometric template is encrypted with the user's secret key. 4. A UID and hash value for the user's biometrics are generated using a

cryptographic hash function, denoted as $H()$, which is used to convert the biometric data vector $\boldsymbol{B}$ into a fixed-length hash value, denoted as $H(B)$. The hash function ensures the integrity and privacy of the biometric data. 5. Finally, create a transaction that includes the UID, $H(B)$, and any additional relevant information.

In order to extract a biometric hash $\boldsymbol{H} = [h_1, h_2, \ldots, h_n]$ with $h_i \in \{0,1\}$ of dimension n, a feature vector $\boldsymbol{a} = [a_1, a_2, \ldots, a_n]$ with $A_i \in R$ is required. Let $\boldsymbol{X^J}$ consist of a subset of x's M ($M < N$)-dimensional features, with potential overlap between features for distinct j. Let $J = 1, \ldots, D$. Let C^J represent a codebook that was created by vector quantising the feature subset $\boldsymbol{X^J}$ using a development set of features $\boldsymbol{X^J}_{(k = 1, \ldots, K)}$. For a given input feature vector $\boldsymbol{X}$, we define $\boldsymbol{h}$ as follows:

$$\boldsymbol{h(X)} = \text{concat}_{J=1,\ldots,D}\left\{\boldsymbol{f}(\boldsymbol{X}^J, \boldsymbol{C}^J)\right\}, \tag{1}$$

where concat(.) stands for the concatenation of binary strings and f is a function that assigns the closest neighbour codewords. The following computations using vector quantisation are made using the codebook C^J. Let $\boldsymbol{X^J}_{(k = 1, \ldots, K)}$ be the development set of feature vector subsets. For a given quantity Q of clusters, the centroids of the underlying clusters are calculated using the kmeans method. Then, centroids are sorted according to how far away from the average of all centroids they are. Finally, binary codewords of size $q = \log_2 Q$ are defined as the position of each centroid in the ranking using grey coding. Finally, broadcast the transaction to the blockchain network based on the range of the UID. The network participants (nodes) validate the transaction and add it to a new block. The miners in the network compete to solve a cryptographic puzzle to append the block to the blockchain. Once a miner successfully solves the puzzle, the block is added to the blockchain, ensuring immutability. For experimental purposes the blockchains were organised by the UID Range. We have considered six blockchain networks, each containing 1000 biometric records.

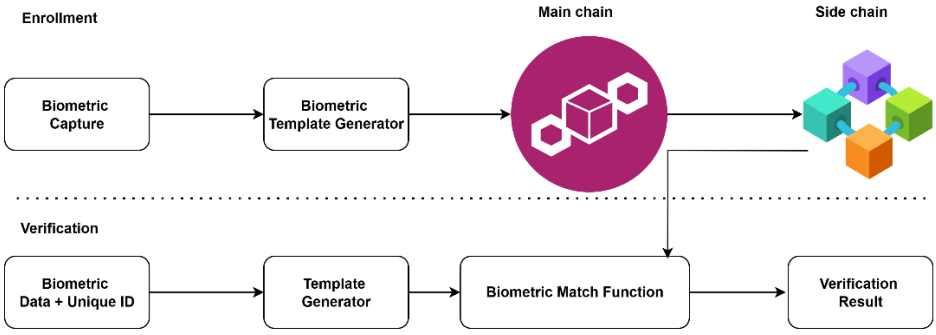

Fig. 2 – *Proposed SBTOS Flow Diagram.*

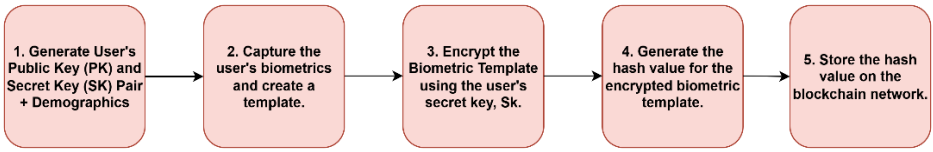

Fig. 3 – *Proposed Solution for Biometric Enrollment.*

Biometric data access on SC plays a vital role, In Uniform access pattern: the biometric templates have the same probability to be accessed by the application irrespective of their previous access time. As a result, in a blockchain, the system should be balanced in terms of query cost and network overhead if every SC has the same number of nodes and each node holds the same quantity of data. Biometric template access pattern that is exponentially decaying: This pattern indicates how long biometric template popularity will last in the actual world. We assume an exponential distribution for the probability of the time until biometric template access happens. The cumulative probability of exponential distribution is given by [28].

$$\mathrm{P}(x,\gamma) = (1 - \mathrm{e}^{-\gamma x}), \quad x > 0, \tag{2}$$

where γ is the rate that establishes the slope's form. The probability of reaching an item by time t is denoted by P(x, γ). Biometric template data availability – If every node in a SC stores the replication of data, then the availability of biometric template data for a SC may be determined from the node availability of members in the SC. It follows that the Poisson distribution is used to express the likelihood that a particular number of nodes will go offline in a specific amount of time with the probability

$$\mathrm{P}(n) = \mathrm{e}^{-\gamma} \frac{\gamma^{n}}{n!}, \tag{3}$$

where n is the number of nodes and γ represents the average rate of nodes to be offline. It is assumed that p is the probability average that the nodes go offline and $\gamma = pn$. If all the nodes on SC go offline, then the biometric data availability across n nodes is given by:

$$\mathrm{P}(BT) = \mathrm{e}^{-\gamma} \sum_{i=0}^{n-1} \frac{\gamma^{i}}{i!}. \tag{4}$$

In a single chain-based system, the mainchain contains all the user's biometric hash values and demographics. In the case of the Aadhar System, which is a centralised BAS for India with 1.3 billion people enrolled, if Aadhar adapts blockchain, then 1.3 billion records have to be migrated to distributed blockchain. Upon storing such a huge number of records on the mainchain, biometric authentication transactions require high resources, gas, and time. To overcome

this issue, the proposed SBTOS uses multiple side chains, in which the users get enrolled by capturing their biometrics and demographics from the client system. Upon successful enrollment, a unique user ID (UID) is issued to the users, which is needed at the verification phase. The biometric authentication phase requires the user's UID and fingerprint on the client side. From the captured user's biometric record, a template is extracted using $H(B)$. The user's biometric template is already enrolled in a side chain that is selected based on the user's UID value range. The extracted template is compared to the user's fingerprint template. Ultimately, the side chain smart contract returns a verification status of either true or false, and the transaction is synchronised with the main chain.

The Sokoto Coventry Fingerprint (SOCOFing) Dataset [33] is used in our work to test the performance of our proposed SBTOS solution. The SOCOFing dataset includes 6,000 fingerprints from 600 African people. Each person has ten fingerprints, and their age is 18+ years old. SOCOFing includes distinctive attributes such as identifiers for gender and hands, as well as digit names. Additionally, synthetically altered variants of these fingerprints are provided with three distinct levels of obliteration, central rotation, and z-cut using the STRANGE Toolkit.

To evaluate the performance of the proposed SBTOS for BAS, a conventional authentication system consisting of a single chain was also implemented using Ethereum blockchain [34], with 6,000 biometric records enrolled. The side chains were implemented using Polygon tool for Ethereum blockchain. To evaluate SBTOS, we have considered six side chains, with each side chain containing 1000 biometric records. We ran both prototypes, and we measured the difference in execution time for biometric authentication. Both systems' backends were implemented using Ethereum version 0.33 and Solidity version 0.8.0. The front-end application is implemented using C# and Windows Forms. The configuration of the system is Windows 11, Intel i5, 16 GB of RAM, and a 512GB SSD. Fig. 4 show the client-side GUI, which contains both enrollment and authentication forms with a biometric preview.

Algorithm 1 Biometric Enrollment in Blockchain Network.

Input: Biometric Raw Image BRI, User Demographics
Output: Hash Value HV
1 Procedure storeBiometric():
2 GenerateKeyPairs ← Pk,Sk
3 CaptureBiometrics || User Demographics ← bytes memory _biometric
4 BiometricTemplate BT← generateTemplate(bytes memory _biometric)
5 UID ← generateUID(String Demographics)
6 EBT ← Encrypt(BT,Sk)

```
7       HV ← HASH(EBT)
8       Select the Blockchain based on UID Range
9       StoreOnLedger ← HV
10      Return UID
Close Procedure storeBiometric():
```

Algorithm 2 Proposed SBTOS Smart Contract.

```
Input: Biometric Raw Image BRI and User ID UID
Output: Authentication True/False
1  Procedure BioAuthenticate():
2       UserRegistered: Contract
3       IsUserRegistered: Boolean
4       AuthenticationStatus: Boolean
5       GenerateKeyPairs ← Pk, Sk
6       CaptureBiometrics ← bytes memory _biometric
7       BiometricTemplate ← generateTemplate(bytes memory _biometric)
8       EBT ← Encrypt(BT,Sk)
9       HV ← HASH(EBT)
10      Read(UID)
11      Select the side chain based on UID Range
12      Mine (HashValue HV of registered user UID in block_Chain[UID-
Range])
13 {
14        If(HashValue HV found Side_Chain[UID-Range])
15    {
16              Print ("User successfully Authenticated")
17              Push ← Broacast the Transaction details in Side_Chain[UID-
Range]
18                                  Push ← Transaction to MainChain
19                                  return AuthenticationStatus==True
 20    }
21  Else
22   {
23      Print("User Authentication Failed")
24   Push ← Broacast the Transaction details in   Side_Chain[UID-Range]
25              Push ← Transaction to MainChain
26              return AuthenticationStatus==False
27        }
28      }
29 CloseProcedure BioAuthenticate():
```

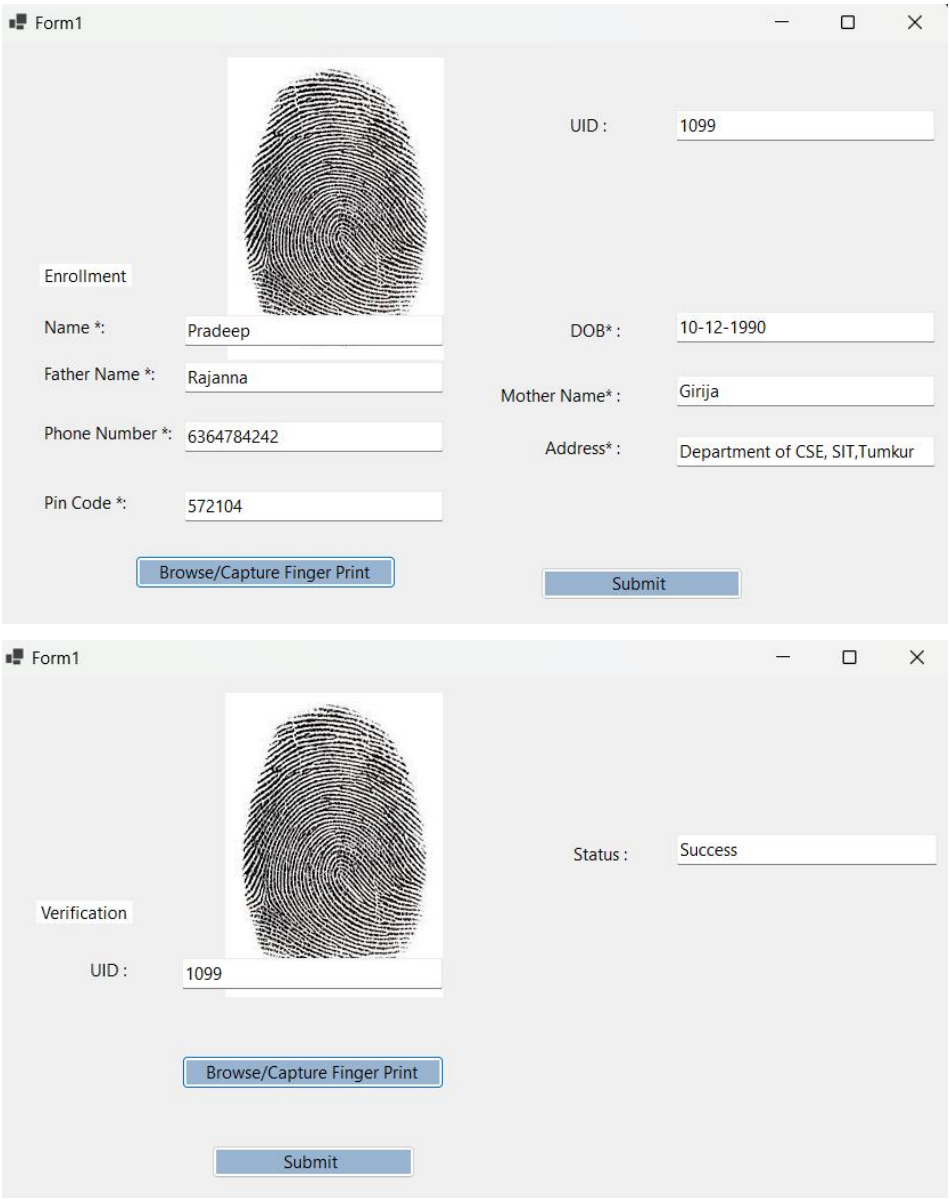

Fig. 4 – *Front End of SBTOS.*

3 Results and Discussion

Fig. 5 compares the biometric enrollment time and Fig. 6 compares the biometric verification times of the legacy single-chain-based BAS and the

proposed SBTOS solution. We evaluated both the systems using the biometric templates, **Table 1** shows the time taken to enrol the biometric templates on both the single chain and SBTOS. The SBTOS takes slightly more time for enrolment due to layered architecture and local sidechain consensus mechanism. The **Table 2** shows the time taken to verify the biometrics on the blockchain systems. The experiment was conducted with increments of 1K biometric templates and the biometric verification times were recorded. Based on the experimental results, it is evident that the SBTOS is a more efficient authentication system than the single chain-based system, as the size of side chains was smaller, and it was able to perform searches and matches quickly.

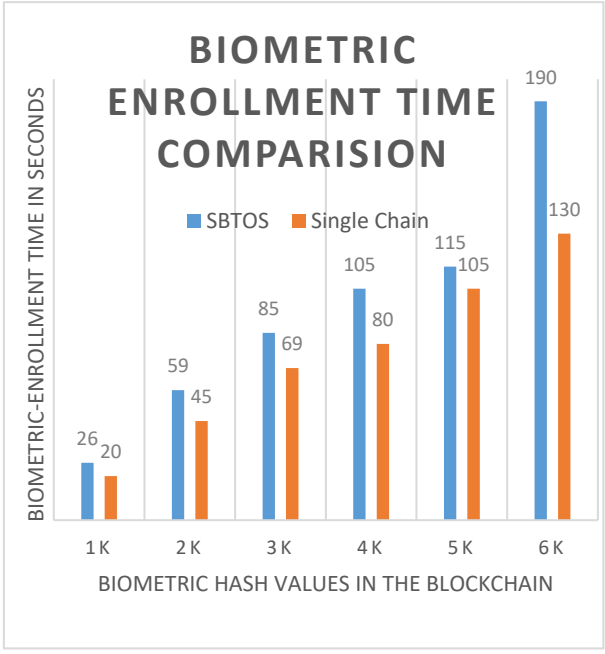

Fig. 5 – *Biometric enrollment time of SBTOS and Single chain BAS.*

Table 1
Biometric Enrollment Time in Seconds.

Biometric Hash	SBTOS	Single Chain
1K	26	20
2K	59	45
3K	85	69
4K	105	80
5K	115	105
6K	190	130

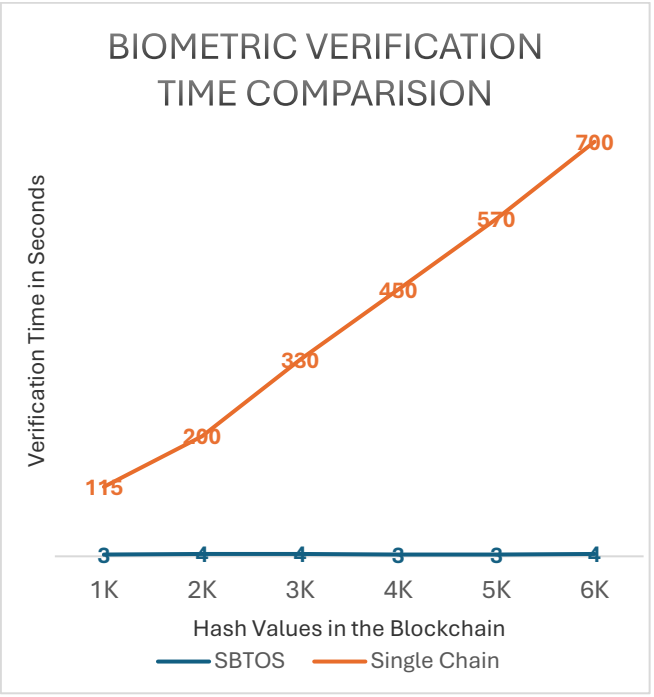

Fig. 6 – *Authentication time of SBTOS and Single chain BAS.*

Table 2
Biometric Verification Time in Seconds.

Biometric Hash	SBTOS	Single Chain
1K	3	115
2K	4	200
3K	4	330
4K	3	450
5K	3	570
6K	4	700

6 Conclusion

In this article, we introduced SBTOS, a novel side chain based biometric authentication transaction optimisation solution that provides decentralised and distributed authentication on the blockchain. SBTOS enhances biometric verification speed, accuracy, and transaction gas consumption compared to single-chain-based BAS by reducing computations at the mainchain. SBTOS solves the single-point failure problem that exists in the client-server model. Through blockchain-based distributed administration and blockchain-based

decentralised authentication, the SBTOS increases the security of biometric data and the reliability and accessibility of authentication activities. SBTOS uses an auditing system built on the blockchain to guarantee the integrity of the transmission of biometric data. The future work involves evaluating the SBTOS with a large quantity of biometric records in the off chains.

7 References

[1] U. Maxsud Tulqin o'g'li: Identification and Authentication, European Journal of Molecular and Clinical Medicine, Vol. 10, No. 1, July 2023, pp. 3869 – 3884.

[2] S. Motamed, A. Broumandnia, A. Nourbakhsh: Multimodal Biometric Recognition Using Particle Swarm Optimization-Based Selected Features, Journal of Information Systems and Telecommunication, Vol. 1, No. 2, June 2013, pp. 79 – 87.

[3] R. Vahedi, S. E. Najafi, F. H. Lotfi: Promote Mobile Banking Services by Using National Smart Card Capabilities and NFC Technology, Journal of Information Systems and Telecommunication, Vol. 4, No. 15, September 2016, pp. 174 – 181.

[4] A. K. Jain, K. Nandakumar: Biometric Authentication: System Security and User Privacy, Computer, Vol. 45, No. 11, November 2012, pp. 87 – 92.

[5] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, F. Roli: Security Evaluation of Biometric Authentication Systems Under Real Spoofing Attacks, IET Biometrics, Vol. 1, No. 1, March 2012, pp. 11 – 24.

[6] I. Pali, L. Krishania, D. Chadha, A. Kandar, G. Varshney, S. Shukla: A Comprehensive Survey of Aadhar and Security Issues, arXiv:2007.09409v1, July 2020, pp. 1 – 12.

[7] A. T. Sheik, C. Maple, G. Epiphaniou: Considerations for Secure MOSIP Deployment, IET Conference Proceedings, Vol. 2022, No. 8, October 2022, pp. 135 – 143.

[8] M. Niknezhad, S. Shokouhyar, M. Minouei: Localization of Blockchain and E-Currency Model for E-Government Services, Journal of Information Systems and Telecommunication, Vol. 8, No. 31, November 2020, pp. 157 – 166.

[9] L. N. Nguyen, T. D. T. Nguyen, T. N. Dinh, M. T. Thai: OptChain: Optimal Transactions Placement for Scalable Blockchain Sharding, Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, USA, July 2019, pp. 525 – 535.

[10] S. Dolinar, D. Divsalar, F. Pollara: Turbo Code Performance as a Function of Code Block Size, Proceedings of the IEEE International Symposium on Information Theory, Cambridge, USA, August 1998, pp. 32 – 32.

[11] J. Eberhardt, J. Heiss: Off-Chaining Models and Approaches to Off-Chain Computations, Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Rennes, France, December 2018, pp. 7 – 12.

[12] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, M. A. Porter: Multilayer Networks, Journal of Complex Networks, Vol. 2, No. 3, September 2014, pp. 203 – 271.

[13] A. Mehrban, P. Ahadian: An Adaptive Network-Based Approach for Advanced Forecasting of Crypto Currency Values, International Journal of Computer Science & Information Technology, Vol. 15, No. 6, December 2023, pp. 1 – 11.

[14] A. Kusum Das: SwarMED: A High-Throughput Interoperability Architecture Over Ethereum and Swarm for Big Biomedical Data, International Journal of Computer Science & Information Technology, Vol. 14, No. 4, August 2022, pp. 31 – 42.

[15] T. T. Anh Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, K.- L. Tan: Blockbench: A Framework for Analyzing Private Blockchains, Proceedings of the International Conference on Management of Data (SIGMOD), Chicago, USA, May 2017, pp. 1085 – 1100.

[16] M. A. Acquah, N. Chen, J.- S. Pan, H.- M. Yang, B. Yan: Securing Fingerprint Template Using Blockchain and Distributed Storage System, Symmetry, Vol. 12, No. 6, June 2020, p. 951.

[17] A. Nourbakhsh, M.- S. Moin, A. Sharifi: Facial Images Quality Assessment Based on ISO/ICAO Standard Compliance Estimation by HMAX Model, Journal of Information Systems and Telecommunication, Vol. 7, No. 27, March 2019, pp. 225 – 237.

[18] I. S. I. Abuhaiba, H. M. Abuthraya, H. B. Hubboub, R. A. Salamah: Image Encryption Using Chaotic Map and Block Chaining, International Journal of Computer Network and Information Security, Vol. 4, No. 7, July 2012, pp. 19 – 26.

[19] P. Mishra, V. Modanwal, H. Kaur, G. Varshney: Pseudo-Biometric Identity Framework: Achieving Self-Sovereignity for Biometrics on Blockchain, Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC), Melbourne, Australia, October 2021, pp. 945 – 951.

[20] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle: Generating Cancelable Fingerprint Templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, April 2007, pp. 561 – 572.

[21] S. M. Hosseini, J. Ferreira, P. C. Bartolomeu: Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and their Limitations, Electronics, Vol. 12, No. 6, March 2023, p. 1283.

[22] O. Delgado-Mohatar, J. Fierrez, R. Tolosana, R. Vera-Rodriguez: Biometric Template Storage with Blockchain: A First Look Into Cost and Performance Tradeoffs, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, USA, June 2019, pp. 2829 – 2837.

[23] H. Chen, M. Pendleton, L. Njilla, S. Xu: A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses, ACM Computing Surveys, Vol. 53, No. 3, May 2021, p. 67.

[24] P. Patil, S. Jagtap: Multi-Modal Biometric System Using Finger Knuckle Image and Retina Image with Template Security Using PolyU and DRIVE Database, International Journal of Information, Vol. 12, No. 4, December 2020, pp. 1043 – 1050.

[25] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan, P. Viswanath: Coded Merkle Tree: Solving Data Availability Attacks in Blockchains, Proceedings of the Financial Cryptography and Data Security: 24th International Conference (FC), Kota Kinabalu, Malaysia, February 2020, pp. 114 – 134.

[26] O. Delgado-Mohatar, J. Fiérrez, R. Tolosana, R. Vera-Rodríguez: Blockchain Meets Biometrics: Concepts, Application to Template Protection, and Trends, arXiv:2003.09262v1 [cs.CV], March 2020, pp. 1 – 16.

[27] W. Yang, W. Ziyang, Z. Xiaohao, Y. Jianming: The Optimisation Research of Blockchain Application in the Financial Institution-Dominated Supply Chain Finance System, International Journal of Production Research, Vol. 61, No. 11, June 2023, pp. 3735 – 3755.

[28] J. W. Heo, G. S. Ramachandran, A. Dorri, R. Jurdak: Blockchain Storage Optimisation with Multi-Level Distributed Caching, IEEE Transactions on Network and Service Management, Vol. 19, No. 4, December 2022, pp. 3724 – 3736.

[29] J. Parra Moyano, O. Ross: KYC Optimization Using Distributed Ledger Technology, Business & Information Systems Engineering, Vol. 59, No. 6, December 2017, pp. 411 – 423.

[30] Z. Zhao, C. Rong, M. G. Jaatun: A Trustworthy Blockchain-Based Decentralised Resource Management System in the Cloud, Proceedings of the IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), Hong Kong, China, December 2020, pp. 617 – 624.

[31] J. A. P. Artiles, D. P. B. Chaves, C. Pimentel: Image Encryption Using Block Cipher and Chaotic Sequences, Signal Processing: Image Communication, Vol. 79, November 2019, pp. 24 – 31.

[32] J. Mahalakshmi, K. Kuppusamy: An Efficient Image Encryption Method Based on Improved Cipher Block Chaining in Cloud Computing as a Security Service, Australian Journal of Basic and Applied Sciences, Vol. 10, No. 2, 2016, pp. 297 – 306.

[33] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, A. James: Sokoto Coventry Fingerprint Dataset, arXiv:1807.10609v1 [cs.CV], July 2018, pp. 1 – 3.

[34] R. Pradeep, N. R. Sunitha: A Reliable Block-Chain Based Biometric Authentication Solution for Aadhar, Indian Journal of Science and Technology, Vol. 15, No. 41, 2022, pp. 2115 – 2120.