International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.027

Blockchain as a Service for Biometric Authentication

Eshwaran S
Department of Computer Science Engineering
Rajalakshmi Engineering College
Chennai, India
eshwaran2001@gmail.com

Charan V
Department of Computer Science Engineering
Rajalakshmi Engineering College
Chennai, India
v.charan621@gmail.com

Pradeep R
Department of Computer Science Engineering
Rajalakshmi Engineering College
Chennai, India
pradeep.r@rajalakshmi.edu.in

ChinnaSakthi K
Department of Computer Science Engineering
Rajalakshmi Engineering College
Chennai, India
sakthisaba@gmail.com

Abstract*— As technology continues to evolve and become more accessible, the need for improved security of data is at an all time high. Biometrics as a form of authentication have been around for quite some time now, but while the technique itself is fairly sound, the way it is implemented can be modified to enhance the system's security. This is where blockchain comes in. By integrating both these technologies, we can minimize the probability of biometric data being leaked or misused while also ensuring that authentication process goes on without any hiccups. Furthermore, offering it as a service will encourage many other services to opt for biometric authentication without having to worry about the security and integrity of the data being stored. By utilizing the concept of smart contracts in our project, we ensure that the project can handle dynamic data and also make sure that the essential conditions are met before the user can utilize our project to enhance the security of their websites. This project will be of immense value to a diverse set of people who need means of providing biometric security to their data but neither have the tools nor the resources to carry it out.

Keywords—Biometrics, blockchain, smart contracts,biometric security.

I. INTRODUCTION

Each and every task done by a human today has been taken over largely by technology. Physical devices like calculators, alarm clocks, maps, compass, etc have been integrated into a single smartphone. This is in a way good as the need for having separate things. But the minority people who have visual impairments find it very difficult to adapt to this technological shift. Also we do not tend to make our advancements friendly to use with for visually challenged people.

Biometric technology has become increasingly prevalent in the past few years. From the fingerprint scanners in our smartphones to iris and voice-based authentication.The technologyhasbecome the defactomeansfor authentication.But the storage of the biometric data has been overlooked by many parties, resulting in sensitive data beingstored in less secure manner. Such data falling into the wrong hands can result in disastrous consequences. This is where integrating blockchain and biometrics becomes a viable solution. The security offered by blockchain technology combined with biometrics can ensure that authentication process goes smoothly while also ensuring that the data itself is a lot more secure.

Biometrics as a Service is already implemented by various companies on different scales. Services such as anonymous face recognition exist, but the data is being stored on third-party cloud services offering SaaS solutions. The challenges of setting up and deploying cloud services have been extensively discussed in the literature. In a cloud computing environment, for example, it may be exceedingly challenging to ensure data privacy while providing quick and secure access, especially in a federated or multi-cloud scenario. Blockchain as a storage is a concept that has been implemented a few times, most popular being InterPlanetary File System (IPFS). All computer devices are intended to share the same file system using a distributed file system called IPFS. The founding objectives of the Web are somewhat comparable, however IPFS is more like a single BitTorrent swarm sharing Git objects.

Our system aims at providing a BlockchainAs A Service for Biometric Authentication (BAAS). The issue with current systems is that they are too complex for certain entities to take advantage of, or they ensure the verification part is secure and smooth, but falters when it comes to secure storage of the biometric data in the system. By utilizing blockchain technologies, we ensure that the biometric data does not get stored with a central entity. It enables web developers to integrate biometric authentication since the decentralisation is applied on the biometrics. It empowers the end users to store the biometric in one entity and use it for authentication anywhere. The block chain provides decentralisation and security for data. Thus the biometric data uploaded by the user remains untampered and unmodified.

II. RELATED WORK

[1] The cost and performance tradeoffs that arise when utilizing public blockchain to store biometrics are analyzed and various techniques of storing the biometrics in a secure and efficient manner are deconstructed in this paper. Some of the techniques

involved include the utilization of smart contracts, data hashing, merkle trees, convolutional neural networks. Storage requirements become very high, thus driving costs up. This is made even more complex by the fact that the value of ether is in constant fluctuation.

[2] A new protocol is put into use that increases the degree of encryption and is "blind," meaning it only shows the identification of a person and no other details about them or their biometric. To achieve this, SVM and neural networks to assign classifier parameters to specific biometric, and authentication is done w.r.t. to that encryption. Multiple communications between client and authentication server, loss in accuracy of biometrics, need for homomorphic encryption scheme increases complexity.

[3] The focus of this paper is to overcome limitations of traditional ballot based voting by uploading user data to the blockchain via smart contract and verifying iris to authenticate into the system. The system complexities are high, given that loss in accuracy of iris data, resulting in users not being authenticated into the system, low success rate due to noise while procuring data from user, variations in data resulting in inconsistencies are present.

[4] Recognition of fingerprint is performed by utilizing Bitmap image and images are converted into templates and then processed. The primary objective is to figure out how biometrics are stored in android device. Trusted Third Party Environment(TTE) is a key component of fingerprint processing in Android devices. The biometrics are encrypted and stored in the isolated environment. But there are chances that if the encrytion key is cracked, then the biometrics can be compromised.

[5] The goal is to implement a facial recognition system that performs face detection and recognition. The color intensity of the image is used for face detection and recognition. The recognition process is performed by implementing geometric features and template matching approaches. Factors such as brightness and contrast affect results, variations based on sensor quality.

[6] A system that eliminates the requirement for a central hub by allowing clients to handle template portions independently and conduct authentication chores on their own. This decentralised strategy makes strong authentication feasible while lowering the likelihood of single-point failures. The first sensor gathers the required biometric information, and then a biometric template is produced. The authenticator assesses if the input and enrolled templates are equivalent, while the administrator manages the registered templates. Each template fragment will be saved randomly selected nodes,not in all nodes.

[7] Despite various security measures being implemented, most of the data are stored in a centralized manner, which can lead to potentially disastrous consequences in the event that security is breached. The cornerstone of this paper is to implement decentralized cloud storage using blockchain technology. This is done by making use of techniques such as IPFS and smart contracts. The sizeof the file and the availability of peers affect how long it takes to upload files.

[8] A novel hybrid model pattern is used to increase the randomness based on the RFID and FingerVein pattern. Thus, they are much more recognisable. They secure the Fingervein and RFID of the patient information using an algorithm and stored in blockchain.

[9] It makes use of a permissioned blockchain technology. Access is necessary in order to join a permissioned blockchain and utilise its functionalities.

[10] It increases the reliability of the data by ensuring that files added to the distributed file system can be tracked and audited. The efficiency, traceability, and security of the IPFS and Ethereum networks are merged in this approach.

[11] A method that provides the iris templates with privacy as well as trust in the calculated output by combining BC technology with encryption. Using Paillier HE in SviaB ensures the privacy of iris templates.

[12] Mitigatation of the security issues prevalent in cloud services by integrating blockchain with the existing service models is done.

[13] A smart contract-based system architecture that combines a multimodal biometric identification system with a permissioned blockchain offers a better form of authentication.

[14] In fingerprint based biometric authentication, the fingerprint data is converted and processed into templates which are split into chunks and stored in the database. During recognition phase the fingerprint template is reconstructed from the broken template and matched.

[15] The major security challenge of blockchain is 51% attacks, where the attackers can rool back the transactions in the side chain and an also hide the information and tractions happening in the main chain. Eclipse attack in the block chain isolates a user from the block chain network, where a attack is performed on user level. The major cause is because a decentralised network does not allow many computers to simultaneously connected all the nodes.

[16] Using a touch-less fingerprint processing chain that reduces the error rate to 1% EER, touchless fingerprints may be compared to those gathered by touch-based fingerprint scanners. FIngerprint scanners work better than mobile fingerprint sensors because of controlled recording condition.

[17] Blockchain can be integrated with the Electronic Healthcare Records (EHRs) to distribute data across healthcare providers thus ensuring the integrity of data. It ensures unique identification of a patient’s records. It ensures security and privacy of healthcare that are exchanged between hospitals and Insurance firms.

[18] Blockchain based storage of EMR(Electronic Medical Records) ensures that the patients records are untampered. Ethereum based smart contracts are used

for data retrieval and viewing permission between patient and the providers.

[19] Blockchain technology can be used in cloud computing to distribute data blocks across clusters of systems. Cloud based mining reduces mining time and at lowcost. Block chain based cloud can be used for payments,data access,etc.

[20] Blockchain Hashing technology can be used for encryption of the files stored in the cloud. The cipher keys are stored and managed in logs similar to ledger in the block chain. It eliminates the presence of the provider in ciphering the files in the cloud.

III. IDEATE

Utilizing biometrics as a method of authentication comes with a few limitations that make the technology in it's current form susceptible to a series of issues. The following are some of the aforementioned issues.

Security risks: Biometric data is sensitive information and can be subject to hackers and data leaks if improperly safeguarded.

Privacy concerns: Storing biometric data raises privacy concerns as well as questions regarding possible identity theft.

Convenience: Users who do not want to share their biometric data or do not have access to the required technologies may find it difficult to save biometric data on a server.

Such issues are mitigated by the utilization of blockchain. Blockchain has key features that are well suited to tackle the issues we observed. Some of these are:

Security: Data saved on networks using blockchain technology are protected using sophisticated cryptography, making it difficult for hackers to access or alter the data.

Decentralization: Data is held among several network nodes rather than in a single central location in decentralisedblockchain networks, which makes it more difficult for a single point of failure to arise.

Transparency: On a blockchain network, all users may see the transparent, unchangeable ledger in which transactions are recorded.

Traceability: Every transaction that takes place on a blockchain network is documented, giving users access to a history of their data that may be used for a variety of purposes, including supply chain management and financial auditing.

Cost-effective: Blockchain technology can reduce costs by doing away with the need for middlemen.

Interoperability: Blockchain networks are capable of exchanging information with other networks and systems, facilitating data sharing and transaction execution across several platforms.

Self-executing smart contracts can automate processes and do away with the need for middlemen, and blockchain networks can make this easier to implement.

Another key aspect of our project is the integration of blockchain and cloud computing. This allows us to provide the project as a service on a wider scale and also handle the large compute power required by blockchain for the mining process. It also enables us to run multiple blockchains in order to store each chunk independently, thereby enhancing data security and integrity.

The advantages of implementing multiple blockchains inside cloud also include:

Flexibility: Using several blockchains allows a more adaptable and flexible storage solution because individual blockchains may be customised for different data kinds and use cases.

Scalability: Due to each blockchain's ability to function independently, scalability may be enhanced, allowing for the processing of more transactions and the storage of more data.

Interoperability: By utilising several blockchains, it might be able to link different blockchain networks and transfer data between them.

Security: By distributing the data among several blockchains, it can be made more challenging for hackers to access or tamper with the information held on the network.

Privacy: Different blockchains can be used to store different kinds of sensitive data, and access to the data may only be granted to those who are authorised.

Another important aspect of our project is the utilization of smart contracts. A smart contract is a self-executing contract with the terms of the agreement recorded in code. The code and the agreements it includes are present on the blockchain network. Automation of processes is made possible by smart contracts, which are frequently used to hasten, guarantee, and enforce contract negotiation and performance. Advantages of smart contracts include:

Automation: Smart contracts streamline operations by automatically carrying out the conditions of the agreement. This decreases the need for middlemen and boosts productivity.

Transparency: Smart contracts are transparent since all parties can see the contents of the agreement and how the contract was carried out because they are both stored on the blockchain network.

Trust: Because smart contracts are executed automatically and the terms of the agreement are recorded on the blockchain network, there is a potential for increased trust between the parties.

Security: Hackers find it challenging to tamper with the agreement or the contract's execution since smart contractsare secured by the blockchain network and the programming that makes up the contract.

Cost-effectiveness: Smart contracts can lower expenses related to middlemen and manual procedures.

Immutable: Once they are recorded on the blockchain network, smart contracts cannot be changed. This

DOI: rp-9788770040723.027

guarantees the validity of the arrangement and the proper performance of the contract.

Efficiency: Since smart contracts self-execute and don't require middlemen, they can speed up the execution of contracts and transactions.

Proposed system over existing system

Currently, blockchain data is kept in databases that the business may own or buy from third parties. Although though using databases to store data is the simplest option, using databases can sometimes cause problems. Databases are often centrally located and maintained by a single entity. They may therefore be more vulnerable to issues like various forms of centralised control and security breaches. This problem is fixed by the widespread adoption of decentralization in blockchain technology.

The fact that they are managed by a network of participants rather than a single institution reduces the negative effects of centralization. This applies to both private and public blockchains. The private blockchains are also decentralized but the number of people who are able to access the blockchain is heavily restricted.

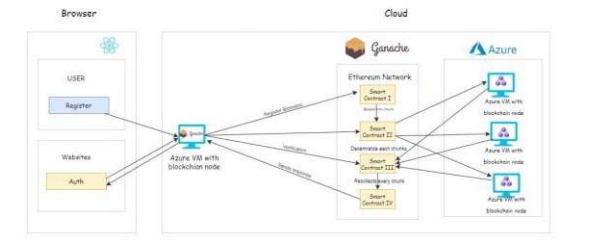
Data integrity issues have plagued databases for a long time. Integrity here refers to the accuracy and consistency of data over a period of time. If the data is not consistent, the system is not trustworthy and dependable. Data integrity in blockchain is ensured by the implementation of Merkle trees. It provides a way to both ensure integrity as well as verify the integrity of the data.

The client has access to the four operations, which are sometimes referred to as the CRUD operations (create, read, update, and delete) in conventional databases. A blockchain is not designed to function similarly to a database. The blockchain technology is related to read and write operations. As the complexity of the system increases, CRUD operations may introduce unnecessary complexity. Such issues are not prevelant in blockchain.

IV. System Design

The project aims at enhancing the security of biometric data by utilizing blockchain to store the data, thereby mitigating a majority of the safety and privacy concerns that exist across multiple alternative implementations of biometric authentication systems.

Architecture



This is the proposed architecture for the project. The system involves maintaining a private blockchain in cloud. Virtual Machines are used to decentralise and maintain the block chain. Biometrics are procured from the user and broken down into chunks. These chunks are decentralised using private block chain maintained across VMs. The developer will be able to integrate the system as service into their websites.

The processes can be divided into two modules. The first module consists of procurement of biometrics. The user registers with the service and enrolls their biometric for storage in the system. The fingerprint is sent to the virtual machine running in the cloud and pushed into the first smart contract, where the biometric is broken down into multiple chunks. These chunks are then pushed into separate blockchains that are isolated from one another and decentralized. This operation is carried out by the second smart contract.

The second module consists of verification and authentication of biometrics. When the fingerprint is required for verification, the client sends a request to the service for authenticating the fingerprint the third smart contract is invoked and fetches the chunks from the blockchain. The chunks are reconstructed into the whole fingerprint template in the fourth smart contract. This is then used to compare and authenticate the fingerprint received from the client for verification.

Smart Contract – 1

The Smart Contract – I takes a biometric template as input and returns encrypted and broken chunks of the biometric template. The broken chunks are given as input to the second smart contract

Smart Contract – 2

This smart contract distributes the data across the virtual machines in the Microsoft Azure cloud. A decentralised private network is maintained across the cloud VMs. Each VM maintains a copy of the blockchain. This smart contract takes each data chunks and stores it in the VM.

Smart Contract – 3

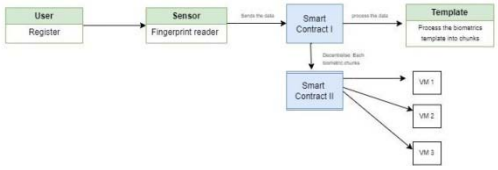
This smart contract fetches the biometric chunks from the VMs. The biometric template is reconstructed from the chunks. The chunks are retrieved based on its hash values. A DTH (Distributed Hash Table) maintains a mapping of the chunk’s hash and its corresponding node’s address that contains the data chunk. Once the chunks are retrieved the biometric template is reconstructed. The reconstruction is done based the order in which the chunks are stored in the DTH table.Thus the smart contract returns the stored biometric template.

Smart Contract – 4

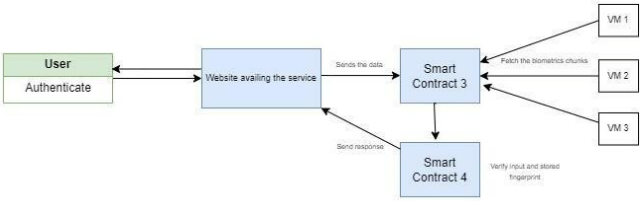
This smart contract accepts the user given biometric and the stored biometric template as input and verifies it. It compares the given biometric against the stored biometric. If the biometrics match then the user is authenticated and a success response is sent to the client. If the biometrics do not match, then the user is not authenticated and a failure reponse is sent back to the client.

DOI: rp-9788770040723.027

System Flow

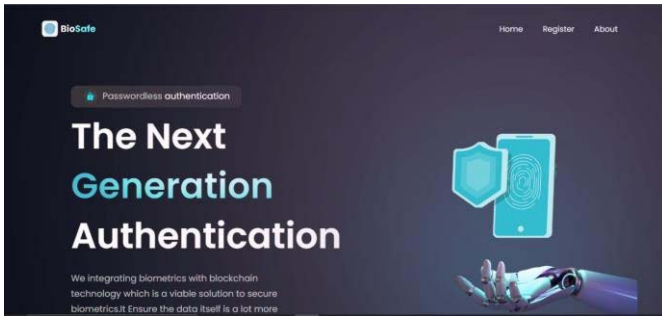


The above diagram showcases the flow of the first module. The user provides fingerprint for registration, and this is forwarded to the first smart contract where it is broken into chunks. Each chunk is then stored in a separate blockchain viathesecondsmartcontract.



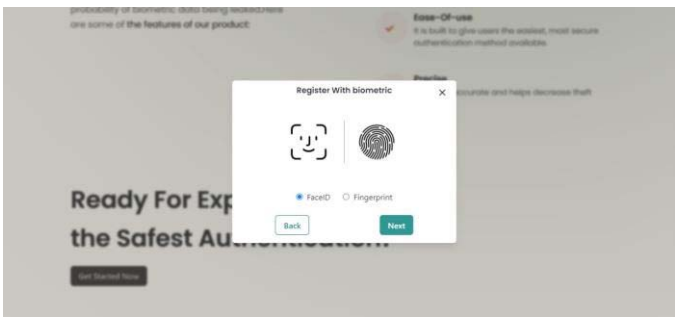
The above diagram showcases the flow of the second module. The client sends the fingerprint to be authenticated. The third smart contract fetches the chunks from the blockchains, and sends them to the fourth smart contract where the fingerprint is reconstructed and used for verification with the fingerprint that was received from the client.

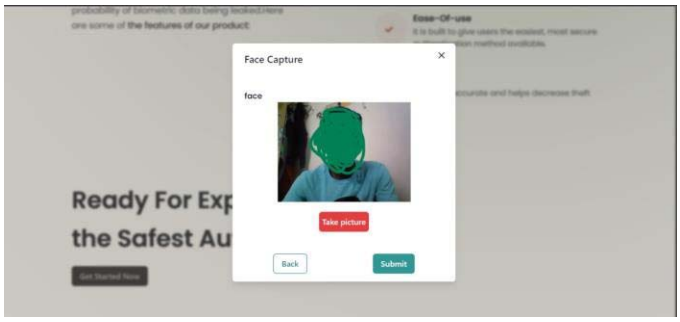
V. IMPLEMENTATION



The home page is where the user can sign up for availing the service by providing their biometric for storage.

After signing up, the user can upload their biometric to the system. The user has the choice between providing facial data or fingerprint data for storage in the blockchain.



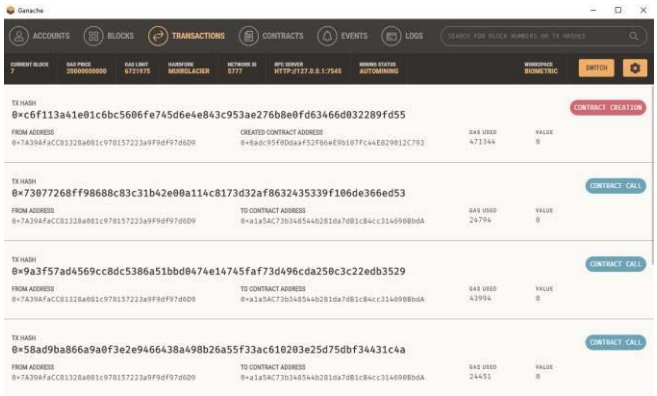


The data is initially supplied to the smart contract when a client delivers a request containing biometric information that has to be validated. A self-executing contract known as a "smart contract" is used to simplify, confirm, and enforce contract negotiations and execution.

As soon as the data enters the smart contract, it is divided into several pieces and stored on several blockchains. It is more challenging for hackers to access or tamper with the data stored on the network due to the decentralisation of data over numerous blockchains, which increases the security and resilience of the system.

Each time a new piece of data is sent, a new block is mined and the chunks are placed inside of it. We keep the data on the Ganacheblockchain, a local blockchain used for testing and development. Both the block's hash and the block that is currently forming are visible. This makes it possible for us to monitor and evaluate the veracity of the data stored on the blockchain.

By segmenting the data and storing it across several blockchains, we can improve the security and integrity of the data and make it more difficult for hackers to access or tamper with it. The Ganacheblockchain also allows us to monitor and verify the accuracy of data.



The biometric authentication system contains an authentication algorithm since it is crucial to the security and precision of the system. Our solution uses a Python-based authentication approach that is run on a Flask server and is created using cutting-edge machine learning algorithms.

When a client wants to utilise the service to authenticate a biometric, they send us a request along with the necessary biometric information. These details are then sent to the server, where they are compared to the data stored on the blockchain. The information on the blockchain is called, put together again, and then compared to validate the user's identity.

A response is delivered to the customer following the conclusion of the verification procedure. The answer will be successful if the biometrics match; otherwise, it will be unsuccessful if the biometrics do not match. This procedure is essential for preserving the security and integrity of the system and for guaranteeing that only authorised users may access it.

VI. Conclusion and Future Work

This paper presented a new biometric authentication system providing a decentralized and distributed authentication based on blockchain. This improves the security and reliability of the existing biometric authentication systems by splitting a biometric template into fragments and managing them based on blockchain mechanism. By implementing both the storage and the authentication of the biometric under the same roof, we avoid the problem of having to send data via the Internet to third party services, which may result in data leakage, putting a huge number of people at jeopardy.

Combining numerous blockchains running on the cloud to construct a biometric authentication system can offer a flexible, scalable, and secure method for storing and managing biometric data. Different types of data can be stored on various blockchains that can be optimised for particular use cases thanks to the use of numerous blockchains. Data decentralisation across several blockchains can increase the system's security and resiliency by making it more challenging for hackers to access or alter the data stored on the network.

Future advancements could use the application of AI and machine learning techniques to enhance the accuracy of the authentication process and to spot and eradicate fraud. Additionally, biometric data can be stored more securelyand privatelyusing zero-knowledgeproofswhilemaintaining the data's opennessandtraceability. Additionally, smart contracts can be used to automatically grant access to the biometric data, ensuring that only those with the right authorization have access to the information. In the future, edge computing can also be integrated into the project. By processing data closer to its source and lowering latency, edge computing can be leveraged to enhance the system's performance and accessibility.

The utilisation of many blockchains operating in the cloud can provide a dependable and safe mechanism for managing biometric data, and this is a promising area for additional research and development.

References

[1] Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana and Ruben Vera- Rodriguez, “Biometric Template Storage with Blockchain: A First Look into Cost and Performance Tradeoffs,” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)

[2] ManeeshUpmanyu, Anoop M. Namboodiri, KannanSrinathan, and C. V. Jawahar, “Blind Authentication: A Secure Crypto-Biometric Verification Protocol,” 2010 IEEE PSPB Operations Manual (sections8.2.1.C & 8.2.2.A).

[3] DiptiPawade, AvaniSakhapara, AishwaryaBadgujar, DivyaAdepu and Melvita Andrade, “Secure Online Voting System Using Biometric and Blockchain,” Advances in Intelligent Systems and Computing, Springer, Singapore, vol. 1042.

[4] Octavian Dospinescu and IlincaLîsîi, “The Recognition of Fingerprints on Mobile Applications – an Android Case Study,” February 2016, Journal of Eastern Europe Research in Business & Economics, pp. 1-11, 2016.

[5] Akanksha,JashanpreetKaur, and Harjeet Singh, Face detection and Recognition: A review Conference: 6th International Conference on Advancements in Engineering & Technology (ICAET-2018).

[6] Meet Shah, MohammedhasanShaikh, Vishwajeet Mishra, and GrinalTuscano, Decentralized Cloud Storage Using Blockchain 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI).

[7] A.H. Mohsin, A.A. Zaidan, and B.B. Zaidan, “A novel verification secure framework for patient authentication,” Computer Standards & Interfaces, vol. 66,2019.

[8] VangaOdelu, “IMBUA: Identity Management on Blockchain for Biometrics-Based User Authentication,”Blockchain and Applications, vol. 1010, 2020.

[9] YounKyu Lee, and JongwookJeong, “Securing biometric authentication system using blockchain,” ICT Express, vol. 7, issue 3, 2021.

[10] Nyaletey, E. Parizi, R.M. Zhang, Q. Choo, K.K.R, “BlockIPFS-Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability,” 2019 IEEE International Conference on Blockchain (Blockchain) At: Atlanta, USA.

[11] Mahesh Kumar MorampudiMunaga, V. N. K. Prasad, Surya NarayanaRajuUndi, SviaB: Secure and verifiable multi-instance iris remote authentication using blockchain, IET Biometrics ,vol. 11, issue 6.

[12] Sitharthan, R., Vimal, S., Verma, A., Karthikeyan, M., Dhanabalan, S. S., Prabaharan, N., ...&Eswaran, T. (2023). Smart microgrid with the internet of things for adequate energy management and analysis. Computers and Electrical Engineering, 106, 108556.

[13] GeetanjaliSawant, and VinayakBharadi, “Permission Blockchain based Smart Contract Utilizing Biometric Authentication as a Service: A Future Trend,” 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW).

[14] S. Hemalatha, “A systematic review on Fingerprint based Biometric Authentication System,” 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).

[15] S. Muralidhara, and B.A. Usha, “Review of Blockchain Security and Privacy,” 2021 5th International Conference on Computing Methodologies and Communication (ICCMC).

[16] Moshika, A., Thirumaran, M., Natarajan, B., Andal, K., Sambasivam, G., &Manoharan, R. (2021). Vulnerability assessment in heterogeneous web environment using probabilistic arithmetic automata. IEEE Access, 9, 74659-74673.

[17] Mohammed al baqari, and EzedinBarka, “Biometric-Based Blockchain EHR System (BBEHR),” 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020.

[18] AsaphAzaria, Ariel Ekblaw; ThiagoVieir,and Andrew Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” 2016 2nd International Conference on Open and Big Data (OBD).

[19] PratimaSharma,MalayaDutta Borah, and Rajni Jindal, “Blockchain Technology for Cloud Storage: A Systematic Literature Review,” ACM Computing Surveys, August 2020.

[20] DhruvDoshi, and SatvikKhara, “Blockchain-Based Decentralized Cloud Storage,” International Conference on Mobile Computing and Sustainable Informatics,January 2021.