International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 377-382, May-2023
https://doi.org/10.47001/IRJIET/2022.602014

Blockchain-based Biometric Authentication System (BBAS) – Secure and Decentralized Approach to Identity Verification

[1]Shubham Metha, [2]Dyuti Dave, [3]Kiran Babu Macha, [4]Prakhar Mittal, [5]Anu Rai

[1]M.S. in Information Systems, Northeastern University, Software Engineer, Northwest Bank, USA
[2]M.S. in Computer Science, Stevens Institute of Technology Technology Analyst, Barclays, USA
[3]University of the Cumberlands, Lead Developer, Maximus Inc, USA
[4]MBA IIM Ahmadabad, Manager Supply Chain, Deloitte USA
[5]Independent Researcher, M.S. in Information Technology and Management, Technical Product Manager, USA

Disclaimer: Authors declare no conflicts of interest. The authors have contributed to this article in their personal capacity without the financial support or review of their employers. As such, the information and opinions in this paper attributable to the author are their own and do not necessarily reflect and are not endorsed by their employers.

Abstract **- Biometric authentication system has been a unique authorization technology which helped us secure data and systems for long period of time. However, with the world transforming digitally and new cutting-edge technologies introduced it has become more prone to cyber attacking, breaches, unauthorized access, and being hacked from any part of the world. This not only leads to access to sensitive data/information but also can possess a national security concern for countries [1] [2]. To address this challenge, introduction and implementation of Blockchain technology is necessary. Blockchain technology's decentralized, transparent and immutable approach can help secure data and manage biometric authentication system. This paper explores the convergence of biometric authentication with blockchain examining how blockchain can enhance data security, ensure user privacy, and provide a tamper-resistant environment for identity verification. This paper also discusses key aspects of blockchain technology, potential uses for different industries, challenges, scalability, functionality, pros & cons, and regulatory compliance. By highlighting the synergy between these technologies, this research aims to shed light on how blockchain can revolutionize biometric authentication, paving the way for more secure and privacy-centric digital ecosystems.**

Keywords: Blockchain technology, biometric, authentication, safety, risks, software systems, technology.

I. Introduction

Information systems have revolutionized the world and changed aspects of human life as we live. A very prominent example is online/offline software services which users use all the time. The main building block of such services is the authentication system of users against the service. We adopted username/password mechanism to fulfill this requirement. However, with the evolution of digital security threats and the increasing need for seamless yet robust authentication, alternative approaches have gained traction.

As technology becomes smarter and advanced so does the risk of it being attacked. We have come a long way from using analog devices like telephone, radio, walkie-talkie to cell phones and now smart phones. As we introduced ourselves digitally to the world, our data became available to world and got into the hands of strangers. As we grow our digital footprint the more it is prone to being accessed and attacked. Biometric authentication systems have been popular since they hold the most natural, unique and distinct combination for every human being. Biometric authentication has a unique cornerstone of secure identity verification by using psychological and behavioral traits. However, traditional centralized systems storing and managing this are prone to attacks like data breach and hacking, exposing sensitive information to unauthorized access and misuse. To address these challenges the integration of blockchain technology offers a groundbreaking approach. Blockchain is decentralized, immutable, and transparent nature provides a robust framework for securing and managing biometric data.

This paper explores the research and study of biometric authentication with blockchain, examining how blockchain can enhance data security, ensure user privacy, and provide a tamper-resistant environment for identity verification. Key aspects discussed include the architecture of blockchain-based biometric systems, potential use cases across industries, and the challenges of scalability, interoperability, and regulatory compliance. By highlighting the synergy between these

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 377-382, May-2023
https://doi.org/10.47001/IRJIET/2022.602014

technologies, this research aims to shed light on how blockchain can revolutionize biometric authentication, paving the way for more secure and privacy-centric digital ecosystems.

II. Background and Related Work

2.1 Biometric Authentication System

Biometric Authentication system is a person's identity-based verification system which uses biological features like fingerprint, facial features, retina scan, voice identification to unlock and access a system. Below are the steps on how it works:

A. Registration:

- User presents a biometric sample such as fingerprints, face scan, etc.
- The system extracts the key features from this biometric scan.
- This extracted information is digital data (basically 1's and 0's) then converted and stored in a biometric template (a mathematical expression).
- This template is then securely stored in a local storage.

B. Authentication:

- User tries to access the system and provides biometric identification.
- The system captures the sample and extracts the important features.
- These features are then compared to the original template.
- Finally, a decision is made based on the threshold.

C. Decision Threshold:

- If the features match the threshold up to a certain level, access is granted.
- If the features don't match, access is denied, and the user must retry or use an alternative authentication method.

Security Measures

- **Liveness Detection:** Prevents spoofing using deepfake detection, pulse detection, or 3D depth analysis.
- **Encryption:** Biometric templates are encrypted to prevent data theft.
- **Multi-Factor Authentication (MFA):** Often combined with passwords or security tokens for stronger security.

Types of Biometric Authentication

- **Fingerprint Recognition:** Uses unique patterns in fingerprints.
- **Facial Recognition:** Analyzes facial features like distance between eyes, nose shape, etc.
- **Iris Recognition:** Scans the unique patterns in the colored ring of the eye.
- **Voice Recognition:** Analyzes voice patterns and speech characteristics.
- **Vein Pattern Recognition:** Uses the unique vein patterns in hands or fingers.
- **Behavioral Biometrics:** Includes keystroke dynamics, gait analysis, etc.

Advantages

- High security (biometric traits are unique and hard to replicate).
- Convenience (no need to remember passwords or carry tokens).
- Fast and efficient authentication.

Challenges

- Privacy concerns (biometric data is sensitive and permanent).
- False positives/negatives (errors in matching).
- Cost of implementation and maintenance.
- Vulnerability to spoofing (e.g., fake fingerprints or photos).

Common Use Cases

- **Mobile Devices:** Face ID, fingerprint unlock
- **Banking & Finance:** Secure transactions, account logins
- **Border Security & Law Enforcement:** Passport control, criminal identification
- **Healthcare:** Patient identification, access control

2.2 Blockchain

Blockchain technology is a decentralized, distributed and transparent system that records each transaction securely across huge network of computer nodes. It works on using cryptographic validation and consensus mechanisms for its smooth, robust, fast and secure work.

A. Block & Chain:

- Block chain is linked blocks which are connected to each other in a LinkedList manner that hold information in cryptographic format. Hence the name Blockchain.
- Each block contains data. This data can be transactions, timestamp, metadata, payload, and a unique cryptographic hash.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 377-382, May-2023
https://doi.org/10.47001/IRJIET/2022.602014

B. Decentralized System:

- Blockchain works on a decentralized system approach where there is no governing mechanism and data is stored across network of computer nodes.
- Each node holds a copy of each blockchain. This is what makes it secure and transparent. So even if one node losesitsdata, other nodes still have the track of a blockchain.

C. Cryptographic Hashing:

- Blockchain uses SHA-256 cryptographic hashing techniques. This is used to hash the previous block, making it secure and tamper resistant.
- If any of this block is altered illegitimately the hash changes, breaking the sync between the nodes and alerting the system.

D. Consensus Mechanism:

- A protocol that ensures all nodes agree on the validity of transactions before they are added to the blockchain.
- This involves Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT).

Types of Blockchains

- **Public Blockchains:** Open to anyone (e.g., Bitcoin, Ethereum). Fully decentralized and transparent to the public.
- **Private Blockchains:** Restricted to specific participants (e.g., used by organizations for internal purposes).
- **Consortium Blockchains:** Controlled by a group of organizations, offering a balance between decentralization and control.

Applications of Blockchain

- **Cryptocurrencies:** Bitcoin, Ethereum, and other digital currencies.
- **Smart Contracts:** Self-executing contracts with terms directly written into code (e.g., Ethereum).
- **Supply Chain Management:** Tracking goods and ensuring transparency.
- **Healthcare:** Securely storing and sharing patient records.
- **Voting Systems:** Ensuring secure and tamper-proof elections.
- **Digital Identity:** Providing secure and verifiable identity management.

Advantages

- **Transparency:** All transactions are visible to participants.
- **Security:** Cryptographic techniques make it highly secure.
- **Immutability:** Data cannot be altered, ensuring trust.
- **Decentralization:** No single point of failure or control.

Challenges

- **Scalability:** Handling a large amounts of transactions quickly.
- **Energy Consumption:** Some consensus mechanisms (e.g., Proof of Work) require significant energy for processing.
- **Regulation:** Legal and regulatory challenges in different jurisdictions.
- **Adoption:** Requires widespread acceptance and integration into existing systems.

2.3 Blockchain for Information System Management

Blockchain advancements and use cases have proven that adopting this technology can be helpful for secure information management. Shafagh et al. demonstrate this concept by utilizing blockchain-based auditable storage for data access [4]. Similarly, Acquah, Chen, Yang, and Yan introduced a blockchain-based fingerprint template within a distributed storage service [5].They proposed that the hash code of the templates can be stored on the blockchain. However, since this is a handshake between the old biometric authentication system and new blockchain technology. Using an old biometric template and storing it into blockchain possess a risk if the template is leaked. This is where this paper proposed a new system that can be completely secure and have no past trials involved for leaks or breaches. Another research study, "Securing Biometric Authentication System Using Blockchain" by Youn Kyu Lee and Jongwook Jeong [6], introduces a novel approach called BDAS (Blockchain-based Distributed Biometric Authentication System). While BDAS effectively addresses several risks associated with traditional biometric systems, it also presents certain limitations, such as performance overhead, scalability concerns, and dependency on blockchain networks.

The proposed BDAS system is a promising approach to enhancing the security and reliability of biometric authentication systems using blockchain technology. However, it has limitations related to performance, scalability, energy consumption, and template segmentation risks. By addressing these limitations through optimization techniques, advanced cryptographic methods, and innovative blockchain

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 377-382, May-2023

https://doi.org/10.47001/IRJIET/2022.602014

architectures, future research can further improve the system and make it more suitable for real-world deployment.

III. Blockchain-based Biometric Authentication System

Blockchain-based systems leverage decentralized, immutable, robust, and transparent framework to enhance security, reliability, and privacy in service for any software, service, and device. These systems are important in scenarios where traditional centralized authentication systems are vulnerable to single points of failure, data breaches, and lack of transparency.

Before diving into authentication, it's essential to understand how blockchain functions. Below is a simple explanation and visualization:

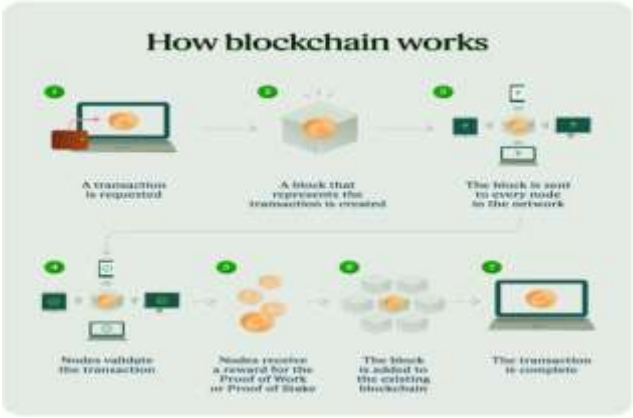

Figure 1: Blockchain working mechanism [7]

Biometric authentication is widely used everywhere nowadays for secure identity verification, but traditional centralized systems face security and reliability issues. The Blockchain-based Biometric Authentication System (BAS) aims to solve existing issues and advance the tech service.

Below, we'll explore how a blockchain-based authentication system works, its functional blocks, and how it addresses future research directions. It also includes a block diagram and sample code for better understanding. It also overcomes and addresses the BDAS Biometric Distributed Authentication System [5].

Functional block Diagram

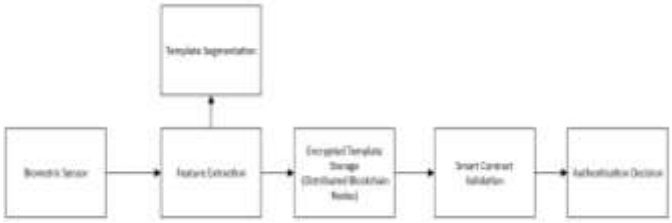

Figure 2: Work flow diagram of BBAS [8]

Workflow of a Blockchain-based Biometric Authentication System

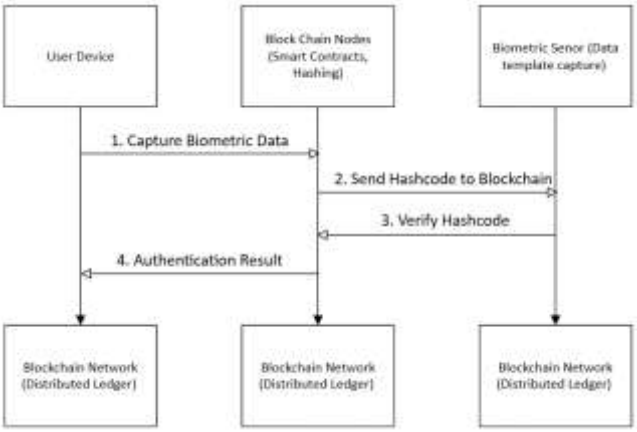

Figure 3: Functional flow diagram of BBAS [9]

1. User Device (Client):

- The user here is the main interacting entity. Users interact with the system through a device which has access to the service.
- The client's device captures biometric information, extracts the features (e.g., fingerprint, facial scan) and sends it to the blockchain network for authentication.

2. Biometric Sensor (Data Capture):

- This sensor captures the user's biometric data (e.g., fingerprint, iris scan, facial recognition) [10].
- It then converts the biometric data into a digital template for processing.

3. Blockchain Node (Smart Contract):

- Executes the authentication logic via smart contracts.
- Verifies the user's biometric template against the stored template on the blockchain.
- Records the authentication transaction on the blockchain ledger.

4. Blockchain Network (Distributed Ledger):

- Stores the hashed biometric templates and authentication transactions.
- Ensures transparency, immutability, and decentralization.

1) Performance Overhead:

- **Issue:** Currently, Blockchain system has latency issues due to consensus mechanisms and transaction recording time.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 377-382, May-2023

https://doi.org/10.47001/IRJIET/2022.602014

- **Solution:**
  - To resolve, we can use off-chain storage (e.g., IPFS) for large biometric data while storing only hashes on the blockchain.
  - Implement layer-2 solutions (e.g., state channels) to handle authentication requests off-chain.
  - Optimize smart contracts for faster execution and efficient work.

2) Scalability:

- **Issue:** As the number of users grows, the blockchain network is becoming congested and hard to manage.
- **Solution:**
  - We can use sharding to divide the blockchain into smaller, more manageable segments. This way we save energy and operations run smoothly.
  - This research also suggests hybrid blockchain models that combine public and private blockchains for scalability.

3) Dependency on Blockchain Networks:

- **Issue:** The system's reliability depends on the number of active nodes at a given point.
- **Solution:**
  - Implementing dynamic node allocation to ensure sufficient nodes are always available. This will work like distributed node network over multipleregions.
  - We can also use redundancy mechanisms to store multiple copies of biometric templates across nodes.

4) Energy Consumption:

- **Issue:** Proof of Work (PoW) blockchains are energy-intensive and consume lot of power for processing even a small transaction.
- **Solution:**
  - Transition to energy-efficient consensus mechanisms like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS).
  - Explore private or consortium blockchains that require less energy.

5) Template Segmentation Risks:

- **Issue:** The current fragmenting biometric templates could be reconstructed if compromised. This can cause data breach or allow illegitimate access to a system.
- **Solution:**
  - Using advanced cryptographic techniques (e.g., homomorphic encryption) to secure template fragments will help a lot.
  - Implementing fragment obfuscation to make reconstruction nearly impossible. This can be achieved by using hashing algorithms and then obfuscating the fragments.

6) Adoption and Deployment Challenges:

- **Issue:** Integrating blockchain systems with existing infrastructure can be challenging.
- **Solution:**
  - Develop interoperability standards for seamless integration.
  - Conduct user studies to improve usability and acceptance.

IV. Conclusion

Integration of Biometric authentication system with Blockchain technology represents a paradigm shift in secure identity verification and authorization. Traditional authentication methods, like fingerprint scanning, voice recognition, retina scan, etc. are vulnerable to cyber threats, data breaches, and unauthorized access. Blockchain technology offers a decentralized, robust, transparent, and immutable nature of transformative approach to mitigating these risks by ensuring enhanced security, data integrity, and user privacy. This research is basically a synergy between blockchain and biometric authentication, highlighting its potential to establish a tamper-resistant, efficient, and scalable authentication framework.

Blockchain-based biometric authentication system (BBAS) not only fortifies security but also addresses long-standing concerns regarding data ownership and privacy. By decentralizing the storage of biometric data and employing cryptographic hashing techniques, blockchain technology significantly reduces the risk of single points of failure and unauthorized manipulation. Furthermore, the integration of smart contracts enhances automation and efficiency in authentication processes, reducing reliance on traditional intermediaries.

Every tech has its pros and cons, the use of blockchain in biometric authentication is no different. Scalability is always of concern, energy-intensive consensus methods, and regulatory uncertainty are significant impediments to wider deployment are few concerns that need to be discussed. However, developing alternatives like layer-2 scaling strategies, hybrid blockchain models, and advances in

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 377-382, May-2023
https://doi.org/10.47001/IRJIET/2022.602014

cryptography methodologies provide intriguing possibilities for overcoming these constraints.

As the digital landscape evolves, the need for safe and privacy-preserving authentication techniques will only increase. The findings of this study highlight the potential for blockchain-based biometric authentication to revolutionize areas such as finance, healthcare, tech, and digital identity management. Future research should concentrate on optimizing blockchain designs, enhancing interoperability with existing authentication mechanisms, and addressing regulatory and ethical concerns in order to promote seamless global deployment. Blockchain-based biometric authentication can pave the way for a more secure, efficient, and decentralized authentication ecosystem, meeting the growing demand for solid cybersecurity solutions in a digital age.

REFERENCES

[1] K. Dharavath, F. A. Talukdar and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," *2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, India, 2013*, pp. 1-7, doi: 10.1109/ICCIC.2013.6724278.

[2] Q. Tao and R. Veldhuis, "Biometric Authentication System on Mobile Personal Devices," *in IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 763-773, April 2010, doi: 10.1109/TIM.2009.2037873.

[3] K. Simoens, J. Bringer, H. Chabanne and S. Seys, "A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems," *in IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 833-841, April 2012, doi: 10.1109/TIFS.2012.2184092.

[4] Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, and Simon Duquennoy. 2017. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. *In Proceedings of the2017 on Cloud Computing Security Workshop (CCSW '17)*. Association for Computing Machinery, New York, NY, USA, 45–50. https://doi.org/10.1145/3140649.3140656.

[5] Acquah, M. A., Chen, N., Pan, J.-S., Yang, H.-M., & Yan, B. (2020). Securing Fingerprint Template Using Blockchain and Distributed Storage System. *Symmetry*, 12(6), 951. https://doi.org/10.3390/sym12060951.

[6] Lee, Y. K., & Jeong, J. (2021). Securing biometric authentication system using blockchain. *ICT Express*, 7(3), 322-326https://doi.org/10.1016/j.icte.2021.08.003.

[7] How Blockchain works: https://www.upwork.com/resources/what-is-blockchain.

[8] Workflow diagram of Blockchain-based Biometric Authentication System.

[9] Functional diagram of Blockchain-based Biometric Authentication System.

[10] A.Singh, R. K. Dhanaraj, M. A. Ali, B. Balusamy and V. Sharma, "Blockchain Technology in Biometric Database System," *2022 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates*, 2022, pp. 1-6, doi: 10.1109/ICCAKM54721.2022.9990133.

Citation of this Article:

Shubham Metha, Dyuti Dave, Kiran Babu Macha, Prakhar Mittal, & Anu Rai, “Blockchain-based Biometric Authentication System (BBAS) – Secure and Decentralized Approach to Identity Verification” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 5, pp 377-382, May 2023. https://doi.org/10.47001/IRJIET/2022.602014

****

