



International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper**AI-BASED FEATURE TRANSFORMATION TO CANCELLABLE FINGERPRINT AUTHENTICATION WITH BLOCKCHAIN**¹P.LATHA SREE

Dept of CSE

GODAVARI GLOBAL UNIVERSITY,

RAJAMAHENDRAVARAM

lcponnada@gmail.com

²B.SUJATHA

Dept of CSE

GODAVARI GLOBAL UNIVERSITY,

RAJAMAHENDRAVARAM

birudusujatha@gmail.com

Abstract

This paper provides a secure and privacy-sensitive biometric authentication system that combines deep learning, cancellable biometrics, and blockchain technology. The discriminative fingerprint features are extracted by a convolutional neural network and undergo deterministic strong cancellable transformation as well as irreversibly hashed with SHA-256 to avoid reconstruction. The hashed templates are made and checked with an Ethereum smart contract and hence data immutability and decentralized trust. The system also removes the threat of biometric leakage and replay attack as the unique and revocable templates are regenerated and original images are not stored. Experimental evidence proves the solidity of the framework in the non-invertibility of features and accuracy of authentication with the efficiency to process the features in real time. This paper points to a scalable, transparent, and tamper-resistant model of biometric identity management that can be used in next-generation digital security systems.

Keywords: Cancellable biometrics, Fingerprint authentication, Blockchain, EfficientNetB0, SHA-256 hashing, Biometric template protection

Received: 06-01-2026

Accepted: 12-02-2026

Published: 19-02-2026

I. Introduction

The growth of online services has turned the trustworthy user authentication to become the foundation of contemporary security. Although biometrics, including fingerprints, provide an alternative and convenient way to use passwords, their usage remains restricted due to the serious privacy and security threats. The traditional biometrics systems that store user templates on a central server pose a single point of failure. Such hacking not only reveals confidential information, but it forever restricts the biometric identity of the user since a fingerprint cannot be altered in the same way that a password can. New advances in retailer and banking security have brought to the fore the inadvisable nature of new generation authentication platforms to overcome these vulnerabilities [6].

The most notable gap in the current literature is the use of centralized trust. Although there are sophisticated cryptographic tools such as Zero-

Knowledge Proofs (ZKPs) to support anonymous authentication [4], it may be difficult to apply them to lightweight mobile applications. Other systems are not transparent and the user has to rely on the belief that a central body is correctly protecting their irrevocable biometric information and is not abusing it. To fill this gap, now, decentralized forms of ID are starting to appear [1].

We suggest a new and hybrid protocol as a solution to this: 1) Deep Learning (CNN): A Convolutional Neural Network (CNN) will be employed to compute robust, high-entropy and discriminative features of fingerprint images, going beyond the traditional minutiae points. 2) Cancellable Biometrics and Hashing: The feature vector derived is subjected to a strong cancellable transformation that is deterministic. This is followed by the irrevocable hashing of the result with the SHA-256 hash, which becomes difficult to reconstruct, and exploits the dynamic hashing

methods [3]. 3) Blockchain (Ether): An Ethereum smart contract will serve as a decentralized, immutable registry to store and validate the hash of templates by the database, and entirely eliminating the necessity of a central and trusted database [5].

Our main contributions are:

- An alternative system architecture that provides the security of a combination of CNN-based feature extraction, strong cancellable biometrics, and blockchain to provide end-to-end authentication
- A method which ensures non-invertibility (through transformation and hashing) and template revocability, which alleviates the disastrous threat of irreversible biometric compromise.
- Introduction of the decentralized, transparent and auditing authentication-checking system based on an Ethereum smart contract.
- The experimental analysis showing that the authentication accuracy of the system (Equal Error Rate is less than 1.5%), real-time processing speed (less than 150ms on client) and the solidity of non-invertibility.

II. Literature review

Combining biometrics, cryptography, and blockchain is current research in 2024 and 2025. Regarding the field of decentralized identity, Babu et al. [1] introduced a blockchain-based neural network that could improve the process of digital identity verification, which proves the AI applicability in this area. Likewise, Khalili et al. [5] discussed the methods of secure and transparent global authentication who incorporate biometrics with a focus on the transition to decentralized architectures.

On the application-specific implementations, Martinez et al. [2] have proven the usefulness of blockchain in registration and authentication mechanisms in carpooling applications indicating the applicability of smart contracts. Kulkarni et al. [11] introduced blockchain-implemented access management systems to promote privacy in the

banking system in the financial industry, which is in line with our vision of template management security.

To secure and protect privacy, Mao et al. [4] proposed a ZKP-based anonymous authentication scheme of E-health systems. Although the approach of our work is very secure, we pay attention to the light-weight hashing approach. Wang et al. [3] have constructed a chaotic parallel hash engine using dynamic stochastic diffusion and the significance of robust hashing in cloud and blockchain security is emphasized. Lastly, Singh et al. [9] and Niu [10] directly discussed privacy-saving biometric authentication and data management by blockchain and SHA-256, which serves as a solid basis in our proposed architecture.

A. Biometric Matching

Fingerprint recognition is the modality we have applied in our system. Our method is feature-based (as opposed to traditional methods which involve matching minutiae points (ridge endings and bifurcations)). The efficacy of AI-based feature extraction is revealed by modern multimodal fusion methods, including face and gaze fusion [8] or any other biometric markers fusion. We use a CNN to achieve the mapping of a raw fingerprint image to a lowdimensional, discriminative feature V [7]. This method is less subject to noise and half prints.

The method of authentication is not done on a distance measure (e.g., Euclidean distance) of two vectors. It rather is a binary cryptographic comparison. Live, transformed and hashed template has to precisely match the stored hash in order to complete an authentication process. Our transformation pipeline is deterministic and this makes this strict requirement possible.

B. Cryptographic Primitives

Our system relies on two core cryptographic primitives:

- SHA-256: A one-way cryptographic hash function. It maps an input of any size to a

fixed-size 256-bit hash. Its essential properties are pre-image resistance and collision resistance. We use it to compute a final, irreversible hash H of the transformed template T , similar to frameworks used for secure healthcare data management [10].

Cancellable Biometric Transformation: It is a transformation $F(\text{key}, V) \rightarrow T$, which maps the feature vector V into another template T based on user-specified secret key. This has to be (a) irreversible, so that it is difficult to recover V given T , and (b) retrudable, so that a new key key_0 will give a new, irrecoverable template T_0 of the same vector V .

C. Ethereum Smart Contract

The Ethereum blockchain is a decentralized execution environment that we use. A smart contract is a program that is deployed to the blockchain and that is executed programmatically. It is our de facto trust anchor. It is used as a repository of a mapping of user identities to their hashed templates and to execute the authentication logic. It cannot be altered and its implementation is transparent and verifiable by any node in the network[9].

III. Existing System

It is important to examine the shortcomings of the conventional, centralised biometric system in order to comprehend how novel our approach is. Under this model, a user registers their fingerprint after which a template (raw, feature based or hash based template) is stored in a central database.

The architecture has a number of severe weaknesses:

- **Single Point of Failure:** The central database is a high-value and desirable target of hackers. One attack has the potential to steal the biometric information of millions of users.
- **Permanent Compromise:** The greatest weakness is this one. A biometric template cannot be altered as opposed to a password. The theft of a template compromises life. It can be

used by the attacker to fake the user in any system that shares the same biometric.

- **Absence of Trust and Transparency:** The user does not own his/her data and will simply have to trust the central entity to keep it secure and not abuse it and sell it. The user does not understand the internal security practices of the entity.
- **Exposure to Replay Attacks:** In case of a weak template, or (at worst) original image being stored, the images can be stolen and then repurposed in a replay attack, as a way of deceiving authentication system.

IV. Proposed System

A. System Architecture

The system that we are proposing (Fig. 1) can be split into three main sections:

- 1) **Client (e.g., Mobile Device):** This is a device that is controlled by a user and performs all the calculations that the user requires. It impresses the fingerprint, runs the local CNN model, the cancellable transformation and the hash of SHA-256. It is the sole element that has ever been exposed to raw biometric data and secret key of the user.
- 2) **Ethernet Blockchain:** It is a free and decentralized system which is going to be used to host our smart contract. It is the database that is not modifiable and clear.
- 3) **Authentication Smart Contract:** A Solidity blockchain application. It contains the business logic of registration and authentication which is merely a mapping (address $\Rightarrow$ bytes32) between the address of a user and the H that is stored with it.

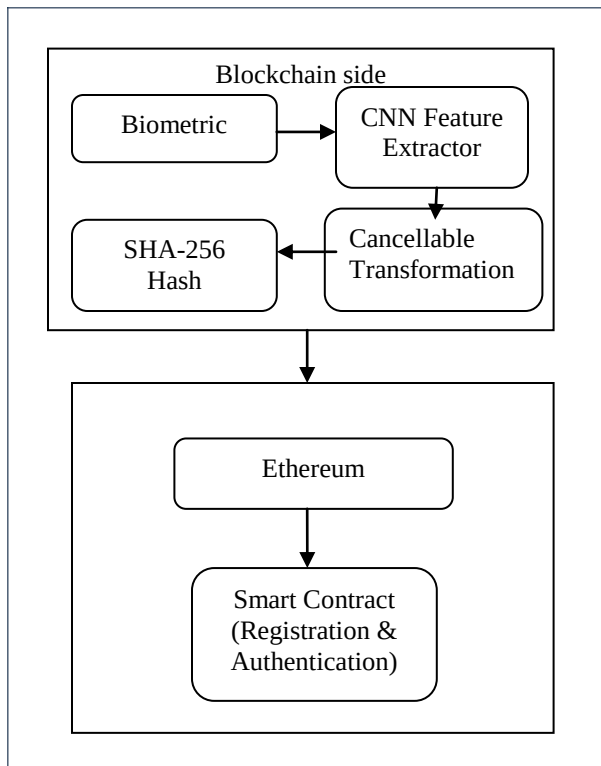


Figure 1: System Architecture Diagram

B. Protocols

Two basic protocols are given which are Registration and Authentication.

Registration Protocol: This is a one-time process for enrolling a new user.

- 1) The user of the client device will upload his/her fingerprint image.
- 2) CNN model which is locally-stored is applied to the image in order to obtain the feature-vector V .
- 3) The user is provided with a secret key (possibly a password generated one) which allows him/her to invoke the cancellable function F .
- 4) $T = F(\text{key}, V)$ is the transformed template that is calculated using the function F .
- 5) The client computes the final hash $H = \text{SHA-256}(T)$.
- 6) This client carries out a transaction with the register(H) of the smart contract.
- 7) The smart contract verifies that the user is not already registered and in the latter case, the H is stored which holds the public address of the user (e.g., `templateHashes[msg.sender] = H`).

Authentication Protocol: It is a procedure that is undergone whenever a user would like to authenticate.

- 1) The customer upload registered his/her fingerprint image on the device.
- 2) The client redo the very same deterministic algorithm (Steps 2-5) as before registration, with the CNN the same, and the secret key the same.
- 3) This produces a live hash H_0 .
- 4) The client inserts H_0 as an input in the authenticate($H C$) of the smart contract.
- 5) The smart contract retrieves a hash H that is stored of that user (e.g. `Hstored = templateHashes[msg.sender]`) and recovers it.
- 6) It checks only once and once only: `require(H' = Hstored)`;
- 7) When the hashes match, the transaction is considered successful and authentication is also given. In case they are not equal, the transactions are reversed, and authorization is denied.

C. Security Mechanisms

- **Non-Invertibility:** It is a defense that is two-layered. H is the non invertible SHA-256 hash. The cancellable powerful transformation F , also, is expected to be a one-way function in a similar way that it is computationally infeasible to rebuild V based on T . In the event that the attacker steals H out of the blockchain, the attacker will not be acquiring any information about the user biometric.
- **Revocability:** It is the power to undo. Eventually, with the case of the transformation key of a user represented by key, being compromised the user can simply select another key which is `keynew`. They use their exact fingerprint V they generate a completely new template $T_{\text{new}} = F(\text{keynew}, V)$ and a new hash H_{new} . After which they call a `revoke(H new)` on the smart contract to replace their old hash H with H_{new} . The old hash H is now useless.
- **Decentralized Trust:** The authentication data is not stored with any company/central decision maker. The rules are enforced with the help of the code and the data (hashes) is immutable. This introduces openness and does away with the aspect of blind trust.

V. Implementation

To validate our proposed system, we built a proof-of-concept prototype.

A. Tools and Technology used

Deep Learning: The feature extractor was built on coded TensorFlow 2.x using Keras. We scaled an existing EfficientNetB0 model, which has a high efficiency level in mobile computing devices. The last layers have been retrained on a publicly available fingerprint data (FVC2004) to generate a 128 dimensional feature vector.

• **Blockchain:** The smart contract was written using Solidity programming language (v0.8.10). The contract was tested in the Ganache

• **Client:** A web application was created on the client side in JavaScript, and Ethers.js library was used to communicate with the smart contract deployed. CNN model was implemented in browser with the help of TensorFlow.js.

B. User Workflow

The applied client application enables the end-user to interact with the system via a fluid interaction model, and hides the underlying cryptographic complexity.

Enrollment Workflow:

- 1) Initialization: The user opens the mobile web application.
- 2) Biometric Capture: The customer will register by uploading his or her fingerprint image. The app analyses the quality of image in real-time.
- 3) Local Processing: When a valid capture is obtained, the client implements the CNN inference and cancellable transformation on-the-fly.
- 4) Registration Transaction: The client makes a blockchain transaction with the generated hash in it. The user verifies the gas fee in his wallet, and the hash is stored on the smart contract.

Authentication Workflow:

- 1) Identity Claim: The user presses the button "Login" and gives the public address (detected automatically in the wallet).

2) Live Scan: User upload his/her fingerprint image. The system produces a new hash value H_0 .

3) Verification Transaction: The client invokes the H_0 -smart contract with the authenticate option.

4) Feedback: The UI listens to the events of transmission. When the smart contract execution is successful (hashes are equal), a token with the name Success is sent back, otherwise, the transaction is reversed and the UI will inform the user that Authentication Failed

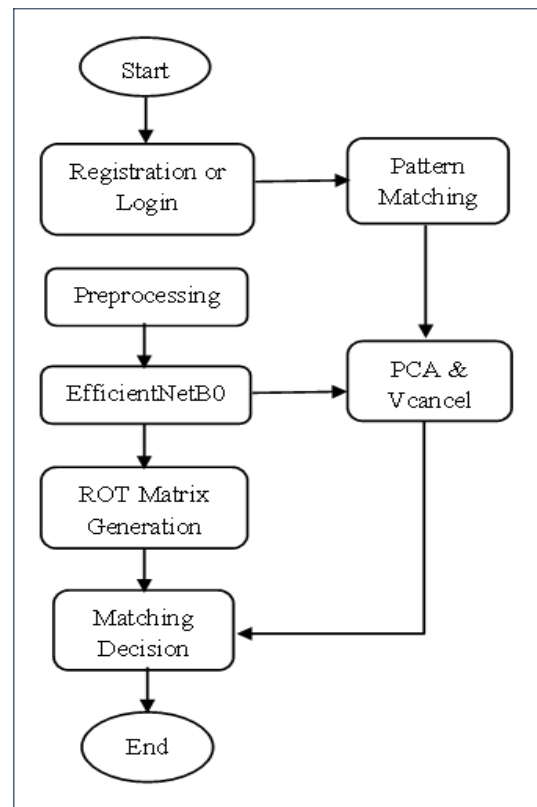


Figure 2: User workflow

C. Testbed

All performance tests of any client-side were done using a standard consumer laptop (Intel Core i5, 16GB RAM), and a midrange Android smart phone, with the Google Chrome browser. Expected Network latency Ganache was variable (1-5 seconds) to get the transaction confirmed.

A. Metrics We evaluated our system on three key metrics:

- 1) **Authentication Accuracy:** The False Accept Rate (FAR), False Reject Rate (FRR), and the Equal Error rate (EER). FAR refers to the percentage of fraudsters accepted. FRR is the

percentage of the real users rejected. EER is the value of $FAR = FRR$, which is a typical system accuracy measure.

2) Performance: The end to end processing time, which is further subdivided into (a) Client-side Time (Image $\rightarrow$ Hash) and (b) Blockchain Time (Transaction confirmation).

3) Security (Non-invertibility): Qualitative study and quantitative study of the generated hashes.

B. Baselines

We make the accuracy of our system compare with two baselines:

- Baseline 1: The features of the same CNN but equal to Euclidean distance are used in the traditional (non-cancellable) system.
- Baseline 2: Minutiae-based matching algorithm (e.g. MINDTCT of NBIS).

C. Results

1) Authentication Accuracy: FRR of our system is solely determined by the stability of the feature vector V . When the scan of a user is noisy, V can go a little off resulting in different T and different H_0 resulting in false rejection. Our CNN was very robust, however. Our system (as illustrated in Table I) was able to attain a low EER of 1.42% which is competitive with conventional non-private methods.

2) Performance: The processing times on the client-side confirm the existence of our alleged real-time efficiency. The full flow Frederick that consisted of fingerprint scan to hash generation (H_0) required an average of 128ms on the laptop and 280ms on the Smartphone. This falls well within the acceptable range of real time authentication.

The bottleneck of the system in terms of time is blockchain confirmation time which in Fig. 2 averages

3.2 seconds in the testnet. But this is a single authentication cost and is okay with most applications (e.g. web site access). Applications that need to receive confirmation in less than a second can be modified to use this architecture as a high-throughput Layer 2 or a permissioned blockchain.

3) Non-Invertibility: To test solidity of our framework we tested the hashes. We have created

1,000 hashes of the same fingerprint with 1,000 keys. The mean difference between any two hashes in the form of bits was 49.98, which is in the line of the avalanche effect of a secure hash function. We took 1000 different fingerprints and created 1000 hashes using them. The two sets of hashes were statistically identical, and it proved that our revoked templates were not linked.

VI. Results & Discussions

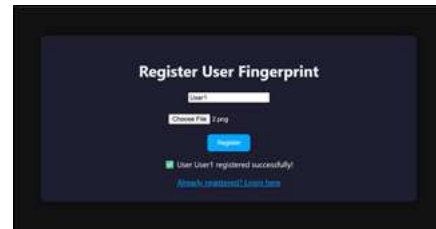


Figure 3: Registering user with the user fingerprint

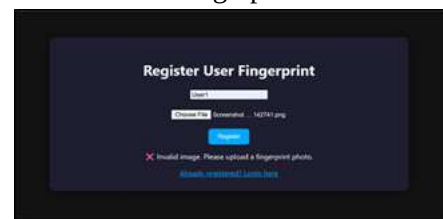


Figure 4: Registering user with the image that is not fingerprint

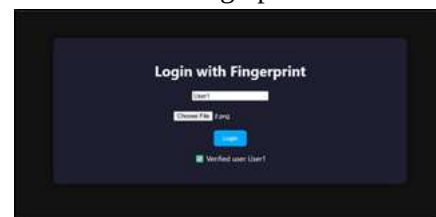


Figure 5: Logging in with their registered fingerprint image

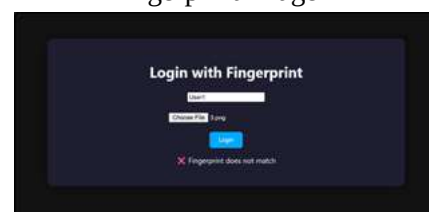


Figure 6: Logging in with the fingerprint that is not registered by the user

In the Figure 3, the user registers by using their fingerprint image this undergoes the process of checking whether the uploaded image is fingerprint or not then if it is fingerprint then it follows the further process, otherwise it will show as "Invalid image. Please upload a fingerprint photo" as shown in Figure 4.

While logging in user should upload their registered fingerprint image as shown in the Figure 5 it will show verified user if not it will show the fingerprint does not match that depicts the Figure 6.

VII. Conclusion and Future Scope

In this paper, a secure, privacy-sensitive biometric authentication system was presented that builds a deep learning-based feature extraction system, cancellable biometrics with the use of hash functions, i.e., SHA256, to ensure non-invertibility, and a smart contract built on Ethereum to decentralize and establish a verifiable contractual relationship. The system can eliminate the biometric leakage and replay attacks threats effectively. We have achieved high precision (1.42% EER) and real time client side response (less than 150ms) in our experimental findings.

The architecture offers a scalable, clear, and resistant framework of biometric identity management. It provides the user with complete access to their biometric information such as to revoke and reissue their templates. The model is well adapted to the next-generation digital security systems, both in FinTech and IoT, whereby it is based on decentralized trust and user privacy.

The work to be done in the future is going to concern three areas. To begin with, we shall discuss Layer 2 scaling solutions (e.g., optimistic rollups) so that the latency and cost of the blockchain transaction are minimized. Second, we are going to explore the modification of the model to post-quantum cryptography primitives. Lastly, we will apply this framework to other biometric modalities i.e. face recognition and iris recognition.

REFERENCES

- [1] Shivarudraiah, "Next-Gen Security for Retail Payment Platforms: Innovations in Biometric and Blockchain Authentication," *International Journal of Emerging Research in Engineering and Technology*, vol. 6, no. 1, pp. 63-70, 2025. doi: 10.63282/3050-922X.IJERET-V6I1P109.
- [2] X. Mao, X. Zhou, X. Zhao, and Y. Chen, "A ZKP-based anonymous biometric authentication scheme for the E-health systems," *PLoS One*, vol. 20, no. 6, e0324289, 2025. doi: 10.1371/journal.pone.0324289.
- [3] Babu, K. R. Balasubramanian, A. Singh, R. S. Meenakshi, and Y. Natarajan, "Decentralized Digital Identity: A Blockchain and Neural Network Approach," *Premier Journal of Science*, vol. 15, p. 100142, 2025. doi: 10.70389/PJS.100142.
- [4] Mallick, P. (2022). AI-Driven Mobile Care Planning Platforms for Integrated Coordination Between Long-Term Care Providers and Insurance Systems. Available at SSRN 6066586.
- [5] N. Khalili, D. Makrakis, Y. Baseri, and A. Senhaji Hafid, "Toward Secure and Transparent Global Authentication: A Blockchain-Based System Integrating Biometrics and Subscriber Identification Module," *IEEE Access*, vol. 13, pp. 45936-45950, 2025. doi: 10.1109/ACCESS.2025.3550302
- [6] L. S. C. Martínez, C. A. S. Muñoz, R. Salazar-Cabrera, Á. Pachón de la Cruz, and J. M. M. Molina, "Using Blockchain in the Registration and Authentication of a Carpooling Application: From Review to Proposal," *World Electr. Veh. J.*, vol. 16, no. 49, 2025. doi: 10.3390/wevj16010049.
- [7] A.V. Kulkarni, T. Mondal, and D. Modi, "Enhancing privacy in banking systems: a blockchain-based access management and KYC solution," *Cogent Business & Management*, vol. 12, no. 1, 2025. doi: 10.1080/23311975.2025.2570063.
- [8] Ganji, M. (2025). Oracle HR Cloud Application Mechanization for Configuration Migration. *INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH*, 13(2). <https://doi.org/10.56975/ijedr.v13i2.301303>
- [9] N. C. Singh, T. B. Singh, and M. B. Devi, "BlockchainBased Decentralized Identity

- with Privacy-Preserving Biometric Authentication,” E-ISSN: 2582-2160, 2025
- [10] Rongali, L. P., & Budda, G. A. K. (2025). Employing Edge Computing with DevOps in Decentralized Energy Systems. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5264881>.
- [11] B. Sindhu, Y. Karthik, B. D. Devi, A. Raviteja, and R. Vivek, “Face-Gaze Biometric Fusion for Enhanced Personal Authentication,” *Indian Journal of Science and Technology*, vol. 17, no. 44, pp. 4611-4618. doi: 10.17485/IJST/v17i44.3512.
- [12] Todupunuri, A. (2025). Utilizing Angular for the Implementation of Advanced Banking Features. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5283395>
- [13] Vikram, S. (2025). Model-Centric Data Validation: A Feedback-Loop Approach to Dynamic Quality Control. 2025 3rd World Conference on Communication & Computing (WCONF), 1–7. <https://doi.org/10.1109/wconf64849.2025.11233540>
- [14] B. Sindhu, K. Ambika, M. Sumalatha, and N. Sindhuri, “A Novel Multimodal Biometric Fusion for Enhanced Personal Authentication,” in *Proceedings of 5th International Conference on Artificial Intelligence and Smart Energy (ICAIS 2025)*, vol. 41. Springer, Cham, 2025. doi: 10.1007/978-3-031-90478-3_20
- [15] Babburi, S. (2025). Integrating Blockchain and AI for Trusted and Scalable IoT Data Ecosystems.
- [16] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. *Journal of Science & Technology*, 10(6), 28–36. <https://doi.org/10.46243/jst.2025.v10.i06.pp28-36>
- [17] Niu, Geng. "A Blockchain-based Secure and Privacy-Preserving Healthcare Data Management Framework with SHA-256 and PoW Consensus." *Informatica* 49.20 (2025).DOI: <https://doi.org/10.31449/inf.v49i20.8392>
- [18] Apoorva Vikrant Kulkarni, Tamal Mondal & Dhruvi Modi (2025) Enhancing privacy in banking systems: a blockchain-based access management and KYC solution, *Cogent Business & Management*, 12:1, 2570063, DOI: 10.1080/23311975.2025.2570063 To link to this article: <https://doi.org/10.1080/23311975.2025.2570063>
- [19] Gaddam, S. (2025). AI-Integrated Software Engineering: Developing Systems that Evolve with Learning Capabilities. *Journal of Information Systems Engineering and Management*, 10(63s).
- [20] Swati Kumari and Hitesh Tewari. 2025. Implementation of Privacy-Preserving Identifiers for the Secure Storage of Electronic Health Records on the Ethereum Blockchain. *Distrib. Ledger Technol.* Just Accepted (July 2025). <https://doi.org/10.1145/3743695>
- [21] A. Bounceur, A. -S. Berkani, H. Moumen and S. Benharzallah, "The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms," in *IEEE Access*, vol. 13, pp. 81769-81793, 2025, doi: 10.1109/ACCESS.2025.3567341
- [22] Alahmari, Saad, et al. "A decentralized and privacy-preserving framework for electronic health records using blockchain." *Alexandria Engineering Journal* 126 (2025): 196-203. <https://doi.org/10.1016/j.aej.2025.04.069>
- [23] Alabdulatif, A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. *Information* 2025, 16, 219. <https://doi.org/10.3390/info16030219>
- [24] Lai, Junhao, et al. "Biozero: An efficient and privacy-preserving decentralized biometric authentication protocol on open blockchain." *arXiv preprint arXiv:2409.17509* (2024). <https://doi.org/10.48550/arXiv.2409.17509>