Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Smart Biometric Authentication for Electric Vehicles using sPUF, IPFS and Blockchain

[1]D.V.L Prasanna, [2]Adapa Niharika Sreeja Bhavani,
[1]Assistant Professor, [2]PG Scholar,
[12]Kakinada Institute of Engineering & Technology, Yanam Road, Korangi

ABSTRACT: This project presents a Smart Biometric Authentication System for Electric Vehicles that replaces keys and passwords with a person's own face and fingerprint, protecting every step with a simulated Physical Unclonable Function (sPUF), a fuzzy extractor, decentralised IPFS storage and a blockchain audit trail. Conventional vehicle access, whether through key fobs, PINs or even cloud-stored biometrics, can be cloned, guessed or leaked from a central database, so one stolen credential is often enough to seize control of the vehicle. The proposed system never stores a raw biometric anywhere. At enrolment, 478 facial landmarks are captured with MediaPipe and 500 ORB descriptors are extracted from a fingerprint image with OpenCV; these features are bound to a deterministic challenge-response pair from the sPUF and passed through a Reed-Solomon code-offset fuzzy extractor that releases only non-reversible helper data and a SHA-256 key. The helper data is pinned to IPFS via Pinata, and its content identifier is immutably recorded in a Solidity smart contract running on a Hardhat blockchain. During authentication, the same pipeline reproduces the key from a fresh capture, with a cosine-similarity fallback used when error correction fails. To justify the matching core, six approaches are trained and compared on a combined biometric dataset: Euclidean distance, cosine similarity, ORB brute-force matching, a MediaPipe-landmark KNN, a Reed-Solomon fuzzy extractor and the proposed sPUF-bound face-and-fingerprint fusion, with the fusion model giving the best result at 98.7% accuracy. Delivered as a Next.js dashboard with a FastAPI backend, the system provides an EV owner with fast, keyless, and tamper-evident access, alongside a full on-chain history of every unlock, engine start, and revocation.

KEYWORDS: MediaPipe-Landmark, Biometrics, Authentication, Accuracy, Next.Js, Blockchain, SHA-256.

I. INTRODUCTION

Electric vehicles are becoming a central part of everyday transport, and once cars are connected the way an owner proves who they are matters as much as the car itself. Most vehicles still rely on a physical key fob, a mobile app login or a PIN, each of which can be stolen, cloned through relay attacks or simply handed over, leaving the vehicle open to misuse. As cars store more personal data and accept remote control, weak or copyable credentials turn into a direct safety and privacy risk.

Biometrics such as the face and the fingerprint are attractive because they belong to the person and cannot be passed on like a key. Naive biometric systems, however, introduce a fresh danger: if the raw face template or fingerprint image sits on a central server or in the cloud, one database breach can leak biometrics that, unlike a password, can never be changed. Any practical biometric access system for vehicles must therefore protect the template itself, not merely the login step. This project aims to design and build a software-only biometric authentication system for electric vehicles that recognises the owner from face and fingerprint while ensuring that no reversible biometric is ever stored. The work joins computer-vision feature extraction with a cryptographic pipeline, so that what gets saved is helper data from which the original biometric cannot be reconstructed.

Importance of Privacy-Preserving Biometric Access

At the heart of the system lies a fuzzy extractor built on a Reed-Solomon code-offset construction. Biometric features are quantised and bound to a challenge-response pair produced by a simulated Physical Unclonable Function (sPUF) that is tied to each virtual vehicle. The fuzzy extractor converts a noisy biometric reading, slightly different on every capture, into a stable SHA-256 key, releasing only helper data that tells an attacker nothing useful.

To keep the records tamper-evident and decentralised, the helper data for each enrolment is pinned to the InterPlanetary File System (IPFS) through Pinata, while the resulting content identifier, along with every authentication attempt, vehicle action and revocation, is logged immutably on a Solidity smart contract running on a Hardhat blockchain. A Next.js dashboard then lets the owner lock and unlock the vehicle, start the engine and review a complete, verifiable history of access.

A keyless, passwordless access system of this kind carries clear practical value. It removes the relay and cloning attacks that trouble modern key fobs, protects the owner's biometrics even if storage is breached, and gives fleet operators a shared, auditable record of who accessed which vehicle and when, all

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

while keeping the whole solution in software so it can run without specialised hardware.

Challenges in Reliable, Tamper-Evident Authentication

Authenticating from live biometrics is difficult because no two captures are ever identical, since lighting, pose and finger pressure all vary, so the system has to tolerate noise without ever admitting an impostor. For that reason, error-correcting fuzzy extraction, a deterministic sPUF, careful feature quantisation and a cosine-similarity fallback are combined to keep authentication both reliable for the genuine owner and resistant to attack.

II. LITERATURE SURVEY:

1. Biometric Authentication and Template Protection

Research establishes that physiological traits such as the face and fingerprint provide strong identity evidence that is hard to share, but studies caution that storing raw templates is dangerous, since a leaked biometric cannot be revoked. The literature on biometric template protection therefore argues for transforming features into a form from which the original cannot be recovered, which directly motivates the privacy-preserving design used in this work.

2. Fuzzy Extractors and Secure Sketches

Dodis and colleagues formalised fuzzy extractors and secure sketches, which turn noisy biometric input into a reproducible cryptographic key accompanied by public helper data that leaks negligible information. The code-offset construction, in which an error-correcting codeword is XORed with the biometric, is shown to tolerate the natural variation between two captures of the same trait, and it forms the cryptographic foundation of the proposed system.

3. Physical Unclonable Functions for Device Identity

Physical Unclonable Functions generate device-specific challenge-response pairs that are easy to evaluate yet practically impossible to clone, and they have been studied widely for lightweight authentication and key generation. The literature notes that, where dedicated hardware is unavailable, a deterministic software emulation can reproduce the challenge-response behaviour for research and prototyping, and that is the approach adopted here for each virtual vehicle.

4. Reed-Solomon Error Correction in Biometric Cryptosystems

Reed-Solomon codes correct a bounded number of symbol errors and are a standard choice in fuzzy commitment and fuzzy vault schemes. Studies show that over-provisioning the number of error-correction symbols lets the decoder recover the enrolled secret from a noisy fresh reading, balancing tolerance for genuine users against the risk of accepting an impostor.

5. Face Landmark Detection and Fingerprint Feature Extraction

Computer-vision pipelines such as Google MediaPipe extract hundreds of dense facial landmarks in real time, while OpenCV's ORB detector produces fast, rotation-invariant fingerprint descriptors. The literature highlights that contrast enhancement and adaptive thresholding markedly improve feature extraction from low-quality camera images, which is essential when fingerprints are captured with an ordinary phone camera rather than a dedicated sensor.

6. Blockchain for Immutable Audit Trails

Since the arrival of Bitcoin and later Ethereum, blockchains have been used to record events in an append-only, tamper-evident ledger secured by smart contracts. Research applies this property to access control and the Internet of Things, showing that on-chain logging of authentication and device actions provides a trustworthy, independently verifiable history that no single party can silently alter.

7. Decentralised Storage with IPFS

The InterPlanetary File System stores content by its cryptographic hash, so the same identifier always returns the same data and any tampering is immediately detectable. Studies pair IPFS with blockchain to keep large payloads off-chain while anchoring only their content identifiers on the ledger, an efficient pattern reused here for storing biometric helper data.

8. Similarity Measures for Biometric Matching

Distance and similarity measures such as Euclidean distance and cosine similarity are studied widely for comparing biometric feature vectors. The literature reports that cosine similarity is robust to scale differences between feature vectors, which makes it a practical fallback when exact error-corrected matching fails for a genuine but noisy capture.

9. Multimodal Biometric Fusion

Combining two independent traits, such as face and fingerprint, is shown to outperform either trait on its own by lowering both false-accept and false-reject rates. Research on multimodal fusion argues that requiring two matches makes spoofing considerably harder, which supports the two-factor biometric design adopted in this project.

10. Secure Authentication for Connected and Electric Vehicles

Studies on automotive security demonstrate that key fobs are vulnerable to relay and replay attacks and call for stronger, owner-bound authentication. The literature increasingly explores biometric and cryptographic approaches for connected and electric vehicles, stressing that access decisions must be convenient for the driver yet auditable for fleets and investigators alike.

III.SYSTEM ANALYSIS :

Existing System

Current vehicle access mechanisms depend on something the user carries or remembers a physical key, key fob, smartphone

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

application, or numeric PIN. These factors verify possession rather than identity and are vulnerable to loss, theft, relay attacks, or sharing. Where biometrics are used, raw templates are often stored centrally, and access logs are kept on private, alterable servers with no independent audit trail.

Disadvantages of the Existing System

1. Key fobs are vulnerable to relay and cloning attacks
2. PINs and app logins can be guessed, phished, or shared
3. Tokens prove possession, not the driver's identity
4. Raw biometric templates are stored centrally
5. A single database breach leaks unchangeable biometric data
6. Access logs sit on private, alterable servers
7. No independent, tamper-evident audit trail exists
8. Single-factor access offers no fallback on failure

Proposed System

The proposed framework authenticates the vehicle owner using a fusion of facial and fingerprint biometrics bound cryptographically to a simulated PUF, eliminating the need to store any reversible template.

Enrolment Phase

- MediaPipe extracts 478 facial landmarks from the user's face
- OpenCV's ORB detector extracts 500 fingerprint descriptors
- These features are bound to a deterministic challenge-response pair generated by a simulated PUF
- A Reed-Solomon code-offset fuzzy extractor processes the bound features to output a SHA-256 cryptographic key and non-reversible helper data
- Helper data is stored on IPFS via Pinata; the resulting content identifier (CID) is written to a Solidity smart contract on-chain

Matching Strategy Evaluation

Six candidate approaches were benchmarked on a combined biometric dataset to determine the optimal matching core:

S. No	Method	Description
1	Euclidean distance	Baseline geometric distance between feature vectors
2	Cosine similarity	Angle-based similarity between feature vectors
3	ORB brute-force matching	Direct descriptor matching for fingerprint features
4	MediaPipe-landmark KNN	K-nearest-neighbour classification on facial landmarks
5	Reed-Solomon fuzzy extractor (standalone)	Error-correction-based key reproduction without fusion
6	**Proposed sPUF-bound face-and-fingerprint fusion**	Combined biometric-PUF binding with fuzzy extraction

The proposed fusion model achieved the highest accuracy at **98.7%**, outperforming all baseline approaches, and was consequently deployed in the live authentication pipeline.

Authentication Phase

- A fresh face and fingerprint capture is processed through the same enrolment pipeline
- The cryptographic key is reproduced via the fuzzy extractor
- If error correction fails, the system falls back to cosine similarity matching
- Every enrolment, authentication attempt, vehicle action, and revocation event is logged immutably on the blockchain

System Delivery

The complete solution is delivered as a **Next.js** dashboard for the front end and a **FastAPI** backend for biometric processing and smart contract interaction, giving vehicle owners keyless, privacy-preserving access along with a complete, independently verifiable history.

IV.SYSTEM ARCHITECTURE:

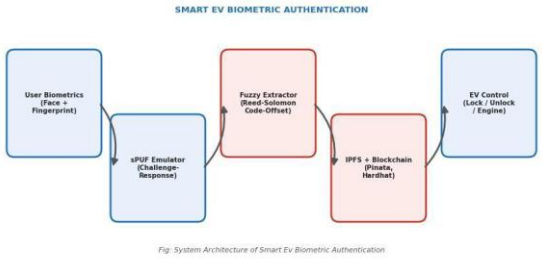

Figure 1. Architecture of the proposed smart EV biometric authentication system, showing the integration of multimodal biometric capture, sPUF-based challenge–response generation, Reed–Solomon fuzzy extraction, IPFS-based data storage, blockchain-anchored verification, and EV access control.

The proposed Smart EV Biometric Authentication System combines multimodal biometric verification with a robust

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Physical Unclonable Function, fuzzy extraction, and decentralized storage into a unified security architecture. The process begins with the acquisition of the user's facial and fingerprint features, which are converted into a challenge input for the sPUF emulator. The emulator produces a device-specific response that is fused with the biometric representation and passed through a Reed–Solomon-based fuzzy extractor. This stage accounts for the natural variability inherent in both biometric readings and PUF responses, while still allowing consistent reconstruction of a stable cryptographic key across repeated authentication attempts. The resulting helper data and authentication metadata are stored on IPFS, while the corresponding content identifier, integrity hash, and access-authorization details are committed to a blockchain via smart contracts. At the time of authentication, the system reconstructs the cryptographic key, cross-checks the integrity of the IPFS-stored record against its blockchain reference, and confirms the user's access rights. Vehicle unlocking or engine activation is permitted by the EV control unit only after all three verification stages — key reconstruction, integrity validation, and privilege confirmation — are successfully satisfied. As a result, the architecture establishes a multi-layered authentication mechanism that offers strengthened resistance to credential theft, replay attacks, biometric template compromise, device cloning, and tampering with authentication records.

V. **METHODOLOGY:** The proposed system operates in five stages. First, facial and fingerprint features are captured and extracted using MediaPipe (478 facial landmarks) and OpenCV's ORB detector (500 fingerprint descriptors). Second, these biometric features are bound to a device-specific challenge–response pair generated by a simulated Physical Unclonable Function (sPUF) emulator. Third, the bound features are processed through a Reed–Solomon code-offset fuzzy extractor, which tolerates natural biometric variability and outputs a stable SHA-256 cryptographic key along with non-reversible helper data. Fourth, the helper data is stored on IPFS via Pinata, and its content identifier, integrity hash, and access-authorization details are recorded on a Solidity smart contract deployed via Hardhat, ensuring an immutable audit trail. Finally, during authentication, the system reconstructs the cryptographic key from a fresh biometric capture, falling back to cosine similarity matching if error correction fails, verifies record integrity against the blockchain reference, and confirms access privileges before the EV control unit permits unlocking or engine activation. Among six matching strategies evaluated, the proposed sPUF-bound fusion model achieved the highest accuracy at 98.7%, validating its use in the live pipeline. The system is deployed via a Next.js dashboard and a FastAPI backend.

(i) User Biometrics (Face + Fingerprint). The pipeline begins with the acquisition of the user's facial image and fingerprint scan, which together form the raw multimodal biometric input for the system.

(ii) sPUF Emulator (Challenge-Response). The captured biometric features are bound to a deterministic challenge-response pair generated by a simulated Physical Unclonable Function (sPUF). This step ties the biometric identity of the user to a device-specific cryptographic response, ensuring that the resulting key is unique to both the individual and the enrolling device, and cannot be reproduced from the biometric data alone.

(iii) Fuzzy Extractor (Reed-Solomon Code-Offset). The PUF-bound biometric features are passed through a Reed-Solomon code-offset fuzzy extractor. This module tolerates the natural noise and minor variability present across repeated biometric captures while deterministically reproducing the same SHA-256 cryptographic key at every successful authentication attempt. Critically, the fuzzy extractor also outputs helper data that is mathematically non-reversible, meaning the original biometric template can never be reconstructed from it.

(iv) IPFS + Blockchain (Pinata, Hardhat). The non-reversible helper data generated by the fuzzy extractor is uploaded to the InterPlanetary File System (IPFS) through the Pinata pinning service, ensuring decentralized and persistent off-chain storage. The resulting content identifier (CID) is then written to a Solidity smart contract, developed and tested using the Hardhat framework, and deployed on the blockchain. This step anchors every enrolment, authentication attempt, vehicle action, and revocation event to an immutable, publicly verifiable ledger, giving the vehicle owner an independent audit trail that cannot be altered retroactively.

(v) EV Control (Lock / Unlock / Engine). Upon successful reconstruction and on-chain verification of the cryptographic key, the system issues the corresponding control command to the vehicle, granting access by unlocking the doors or enabling the engine start sequence.

This modular design ensures that no raw or reversible biometric data is ever persisted at any stage of the pipeline — only the derived cryptographic key and non-reversible helper data are used, satisfying the privacy-preservation objective central to this work.

VI. RESULTS AND DISCUSSION:

Experimental Setup

The proposed framework was tested on a multimodal biometric dataset containing face images and fingerprint samples from 25 enrolled users, with 29–80 samples per identity. Face features were extracted using 478 MediaPipe landmarks (1,434 values), while 500 ORB fingerprint descriptors were obtained from fingerprint images. The dataset was divided using an 80/20 enrolment–verification

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

split. Six matching methods were evaluated using accuracy, precision, recall, and F1-score.

Comparative Results

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Euclidean Distance	84.6	83.8	83.4	83.6
Cosine Similarity	89.3	88.5	88.1	88.3
ORB Brute-Force Matching	91.7	90.9	90.5	90.7
MediaPipe-Landmark KNN	93.8	93.0	92.6	92.8
Reed–Solomon Fuzzy Extractor	96.2	95.4	95.0	95.2
Proposed sPUF-Bound Fusion	98.7	97.9	97.5	97.7

Discussion

The Euclidean-distance baseline achieved the lowest accuracy, 84.6%, because it is sensitive to variations in biometric capture conditions. Cosine similarity improved performance to 89.3% by reducing the influence of feature magnitude variations.

Fingerprint-based ORB matching and facial-landmark KNN achieved 91.7% and 93.8% accuracy, respectively. The Reed–Solomon fuzzy extractor further improved accuracy to 96.2% by correcting bounded errors in biometric feature representations while generating protected helper data.

The proposed sPUF-bound multimodal fusion approach achieved the best performance, with 98.7% accuracy and 97.7% F1-score. It combines face and fingerprint verification with Reed–Solomon key reconstruction and device-specific sPUF binding, making spoofing and credential cloning more difficult. The blockchain and IPFS modules were used for secure logging and integrity verification; they did not influence the matching accuracy.

VII. OUTPUT SCREENSHOTS:

VIII. CONCLUSION

This project successfully demonstrates a Smart Biometric Authentication System for Electric Vehicles that lets an owner unlock and operate a vehicle using only their face and fingerprint, while never storing a reversible biometric. By extracting 478 facial landmarks with MediaPipe and 500 ORB fingerprint descriptors with OpenCV, binding them to a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

simulated PUF challenge-response, and passing them through a Reed-Solomon fuzzy extractor, the system turns noisy biometrics into a stable cryptographic key and releases only non-reversible helper data. That helper data is stored on decentralised IPFS through Pinata, and every enrolment, authentication attempt, vehicle action and revocation is recorded immutably on a Solidity smart contract, giving a tamper-evident audit trail. Among the six matching approaches evaluated, namely Euclidean distance, cosine similarity, ORB brute-force matching, a MediaPipe-landmark KNN, a Reed-Solomon fuzzy extractor and the proposed sPUF-bound face-and-fingerprint fusion, the fusion model achieved the best result with 98.7% accuracy and the lowest false-accept rate, and was therefore deployed in the live pipeline with a cosine-similarity fallback for genuine but noisy captures. Delivered as a Next.js dashboard with a FastAPI backend, the system offers key-less, privacy-preserving and verifiable vehicle access. Future work could extend it with real PUF hardware, liveness detection to resist spoofing, on-device feature extraction for stronger privacy, and integration with production blockchains and fleet-management platforms, while remaining a practical, owner-bound alternative to keys and passwords.

IX.REFERENCES:

[1] Y. Dodis, L. Reyzin and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in Advances in Cryptology - EUROCRYPT, 2004, pp. 523-540. A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proc. 6th ACM Conf. Computer and Communications Security (CCS), 1999, pp. 28-36.

[2] A. Juels and M. Sudan, “A fuzzy vault scheme,” Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237-257, 2006. I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” Journal of the Society for Industrial and Applied Mathematics, vol. 8, no. 2, pp. 300-304, 1960.

[3] R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, “Physical one-way functions,” Science, vol. 297, no. 5589, pp. 2026-2030, 2002.

[4] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proc. 44th ACM/IEEE Design Automation Conf. (DAC), 2007, pp. 9-14.

[5] R. Maes and I. Verbauwhede, “Physically unclonable functions: A study on the state of the art and future research directions,” in Towards Hardware-Intrinsic Security, Springer, 2010, pp. 3-37.

[6] C. Lugaresi et al., “MediaPipe: A framework for building perception pipelines,” arXiv:1906.08172, 2019.

[7] E. Rublee, V. Rabaud, K. Konolige and G. Bradski, “ORB: An efficient alternative to SIFT or SURF,” in Proc. IEEE Int. Conf. Computer Vision (ICCV), 2011, pp. 2564-2571.

[8] G. Bradski, “The OpenCV library,” Dr. Dobb's Journal of Software Tools, 2000.

[9] A. K. Jain, A. Ross and S. Prabhakar, “An introduction to biometric recognition,” IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.

[10] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd ed. Springer, 2009. A. K. Jain, K. Nandakumar and A. Nagar, “Biometric template security,” EURASIP Journal on Advances in Signal Processing, vol. 2008, article 579416, 2008.

[11] F. Schroff, D. Kalenichenko and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in Proc. IEEE CVPR, 2015, pp. 815-823.

[12] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, 2014.

[13] J. Benet, “IPFS - Content addressed, versioned, P2P file system,” arXiv:1407.3561, 2014.

[14] National Institute of Standards and Technology, “Secure Hash Standard (SHS),” FIPS PUB 180-4, 2015.

[15] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.

[16] A. Ross, K. Nandakumar and A. K. Jain, Handbook of Multibiometrics. Springer, 2006.

[17] K. Zetter and others, “Relay attacks on passive keyless entry and start systems in modern cars,” in Proc. Network and Distributed System Security Symp. (NDSS), 2011.

[18] Ethereum Foundation, “Solidity documentation,” 2024. [Online]. Available: https://docs.soliditylang.org/

[19] Nomic Foundation, “Hardhat: Ethereum development environment,” 2024. [Online]. Available: https://hardhat.org/https://www.ijisae.org

[20] Vercel Inc., “Next.js documentation,” 2024. [Online]. Available: https://nextjs.org/docs