Secure Digital Certificate Verification Using Blockchain, Facial Biometrics, And Hybrid AES-ECC Encryption

Akkash Deep. V[1], Ragul. N[2], Mohammed Gani. H[3], Saktheeshwaran .M[4], Dhamodharan. V[5]
[1, 2, 3, 4] Dept of Artificial Intelligence and Data Science
[5]Assist prof, Dept of Artificial Intelligence and Data Science
[1, 2, 3, 4, 5] MAMCET, Tamil Nadu, India

Abstract- *Digital certificate management faces persistent threats including forgery, unauthorised access, and data manipulation. Conventional centralised systems are vulnerable to single-point failures, poor scalability, and weak identity verification. This paper proposes a secure certificate verification framework integrating three complementary layers: facial biometric authentication using the Grassmann manifold algorithm, hybrid encryption combining AES-256 for bulk file protection and Elliptic Curve Cryptography (ECC) for secure key management, and a blockchain-based decentralised immutable ledger for certificate storage. One-Time Password (OTP) delivery and SHA-256 hash validation reinforce access control at every stage. A Flask-Python web prototype demonstrates end-to-end certificate issuance, encrypted storage, biometric-gated retrieval, and third-party verification. The system eliminates dependence on centralised infrastructure, provides tamper-proof transparency, and scales efficiently across multiple institutions.*

Keywords: AES-ECC Encryption, Blockchain, Certificate Verification, Elliptic Curve Cryptography, Facial Biometrics, Grassmann Algorithm, OTP Authentication

I. INTRODUCTION

The growing shift towards digital academic and professional credentials has made secure certificate management a critical concern. Traditional paper-based certificates are easily forged, damaged, or lost, while digitised versions stored on centralised servers remain exposed to hacking, insider threats, and single-point failures [1]. Credential fraud in higher education and corporate recruitment continues to grow, undermining institutional trust globally.

Existing digital verification approaches rely primarily on QR codes or basic OTP systems, which offer limited resistance against sophisticated attacks and struggle to scale across multiple institutions. Centralised storage of biometric data also raises significant privacy concerns under modern data-protection regulations.

To address these gaps, this paper presents a unified framework that integrates: (i) Grassmann manifold-based facial biometrics for accurate identity verification, (ii) a hybrid AES-ECC encryption scheme offering both speed and cryptographic strength, and (iii) a blockchain ledger for decentralised and tamper-proof certificate storage. Supplementary OTP delivery and SHA-256 hash validation provide defence-in-depth access control.

II. LITERATURE SURVEY

Chotijah et al. [2] proposed a blockchain-based e-certificate system using smart contracts for automated issuance and revocation, achieving near-instant verification. However, the absence of biometric binding leaves the system vulnerable to impersonation attacks.

A multi-case study [3] confirmed that distributed ledger adoption improves transparency and reduces administrative overhead in credential management, while identifying scalability under heavy transaction loads as an open challenge.

Alansari et al. introduced GhostFaceNets [4], lightweight deep models for edge-device face recognition. Deng et al. proposed ArcFace [5], an additive angular-margin loss achieving state-of-the-art accuracy on large-scale face benchmarks. Both confirm the maturity of deep biometric pipelines but do not address certificate management integration.

RetinaFace [6] demonstrated robust multi-scale facial localisation under occlusion and illumination variations. Edwards et al. presented Fossil 2.0 [7], a formal certificate synthesis framework emphasising cryptographic correctness proofs. A controlled blockchain correction mechanism in [8] showed how audit trails balance immutability with practical error-handling. None of these works unifies biometrics, hybrid encryption, and blockchain into a single pipeline, which is the contribution of this paper.

III. PROPOSED METHODOLOGY

3.1 Proposed System

The framework involves three actors — Institution, Student, and Verifier — interacting across seven modules over a Flask-Python backend with MySQL storage and a blockchain ledger. Certificates pass through an unbroken chain of cryptographic protections from issuance to third-party verification.

Advantages

- Provides high-level security using hybrid AES and ECC encryption for dual-layer data protection.
- Enhances identity verification with accurate facial recognition via the Grassmann algorithm.
- Ensures tamper-proof, transparent, and

Traceable certificate storage through blockchain technology.

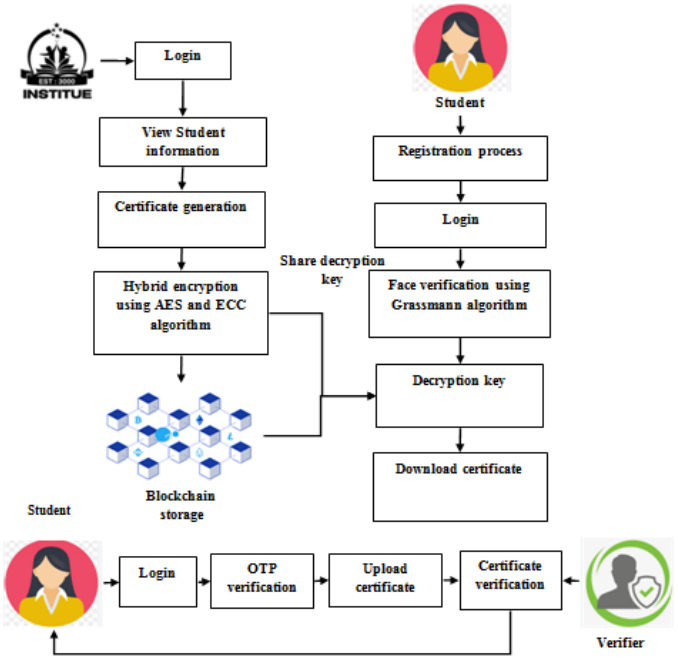

Fig. 1: Proposed Architecture Diagram

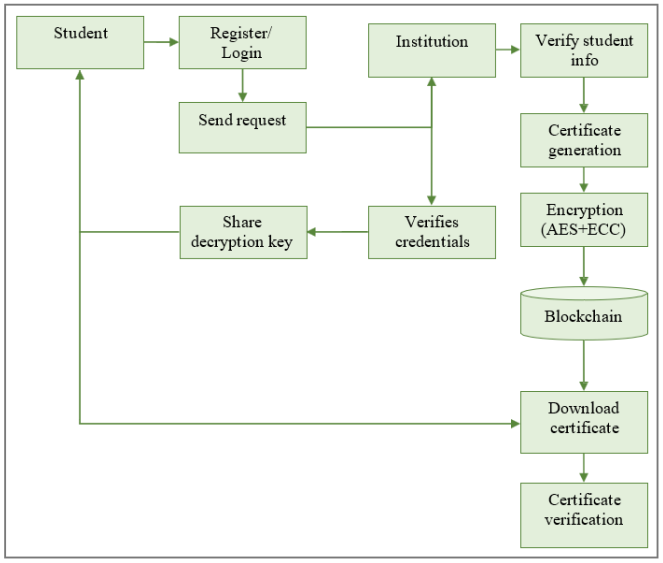

Fig. 2: Proposed Block Diagram

IV .SYSTEM REQUIREMENTS

4.1 Hardware Specifications

- Processor: Dual core processor 2.6.0GHZ
- RAM : 4GB
- Hard disk : 320 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor :15 inch color monitor

4.2 Software Specifications

- Operating system: Windows OS
- Front End : Html, CSS, JAVASCRIPT
- Back End : Python
- Data base : MySQL SERVER
- IDLE : Python 2.7 IDLE

V. MODULE DESCRIPTION

Framework Creation Module*:* Initialises database schemas, user roles, access-control policies, encryption parameters, and blockchain connection settings. Sets up logging and audit infrastructure.

Institution Process Module*:* Authorised personnel upload student certificates. The module validates completeness, assigns unique document identifiers, and queues files for encryption.

File Encryption Module (Hybrid AES-ECC)*:* Each certificate is encrypted with a randomly generated AES-256

key. The key is then encapsulated with the recipient's ECC public key (secp256k1), producing a compact ciphertext bundle combining bulk-encryption speed with asymmetric key-management security.

Blockchain Storage Module: Encrypted bundles and SHA-256 digests are committed as immutable blockchain transactions, time-stamped and signed by the issuing institution node to ensure non-repudiation.

User Authentication Module*:* Login triggers credential checking followed by live facial verification via the Grassmann algorithm, which projects face embeddings onto a Grassmann manifold and measures geodesic distances for identity matching. A concurrent OTP serves as the second factor.

Decryption and Download Module*:* Authenticated users submit their ECC decryption key; the system verifies the SHA-256 digest, decrypts the AES key, and reconstructs the original certificate for download.

Verifier Process Module*:* External verifiers upload a certificate; the system recomputes its SHA-256 hash and compares it against the blockchain record, returning an Original or Fake verdict.

VI. SYSTEM IMPLEMENTATION

6.1 UML Diagrams

UML diagrams capture the static structure and dynamic behaviour of the proposed system. The use case diagram (Fig. 3) identifies actors and system functions. The class diagram (Fig. 4) defines entity relationships and module interfaces. The sequence diagram (Fig. 5) traces the message flow for certificate issuance and retrieval. The activity diagram (Fig. 6) maps the decision logic for authentication and verification.

6.2 USE CASE DIAGRAM

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. In this context, a "system" is something being developed or operated, such as a web site. The "actors" are people or entities operating under defined roles within the system.

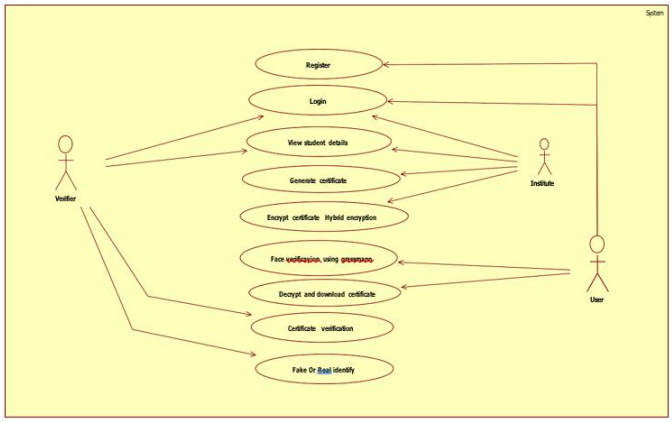

Fig. 3: Use Case Diagram

6.3 CLASS DIAGRAM

A class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations and the relationships among objects. The class diagram is the main building block of object-oriented modeling. It is used for general conceptual modeling of the systematic of the application, and for detailed modeling translating the models into programming code.

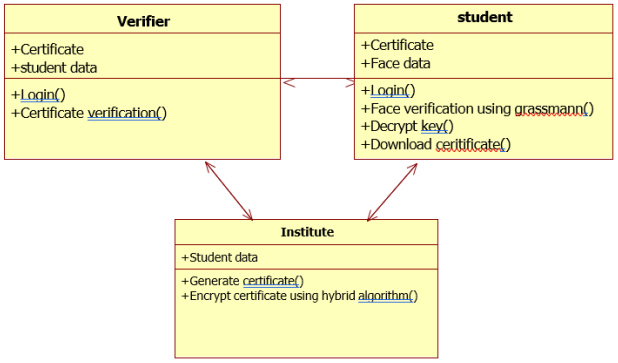

Figure 2.4: Class Diagram

Fig. 4: Class Diagram

6.4 SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

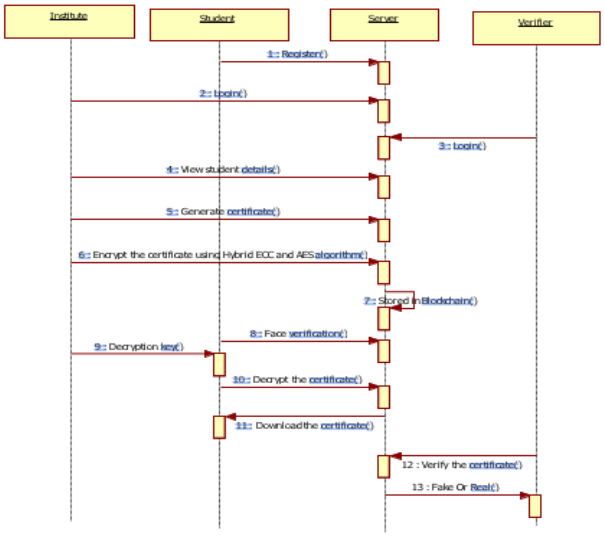

Fig. 5: Sequence Diagram

6.5 ACTIVITY DIAGRAM

Activity diagram displays a special state diagram, where most of the states are action states and most of the transitions are triggered by completion of the action in the source states. The activity can be described as an operation of the system. So the control flow is drawn from one operation to another. This flow can be Fig. 6: Activity Diagram sequential, branched or concurrent. Activity diagrams deals with all type of flow control by using different elements.

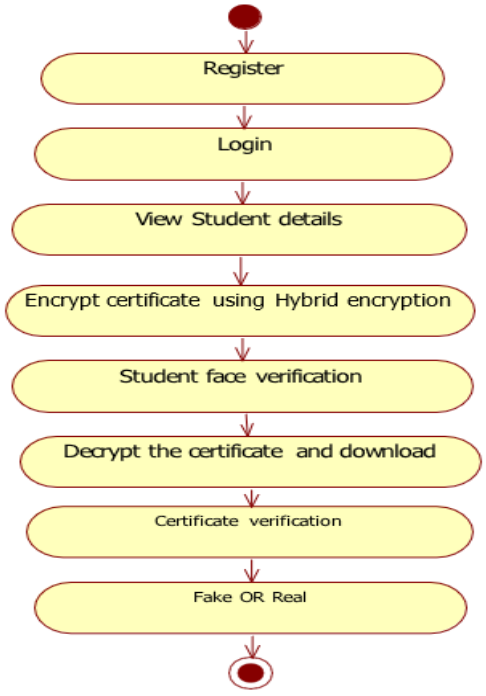

Fig. 6: Activity Diagram

VII. VERIFICATION AND VALIDATION

7.1 Verification: Confirming Authenticity

The verification framework is built to guarantee that every certificate is genuine, immune to tampering, and linked exclusively to its rightful owner. Stakeholders—such as potential employers, universities, or government bodies—can verify a document instantly by scanning a QR code or querying the blockchain directly. Because each record is stored as a unique, encrypted entry on the decentralized ledger, its origin and integrity are indisputable.

Security during verification is multi-layered:

Biometric Identity: The system utilizes facial recognition powered by the Grassmann algorithm to ensure the person presenting the credential is who they claim to be.

Access Control: One-Time Passwords (OTP) and unique hash keys act as digital gatekeepers, preventing unauthorized parties from intercepting the process.

Transparency: Every request is time-stamped and logged, creating a permanent audit trail. Since the blockchain relies on node consensus, the data cannot be altered after the fact, making the verification process both scalable and highly resistant to fraud.

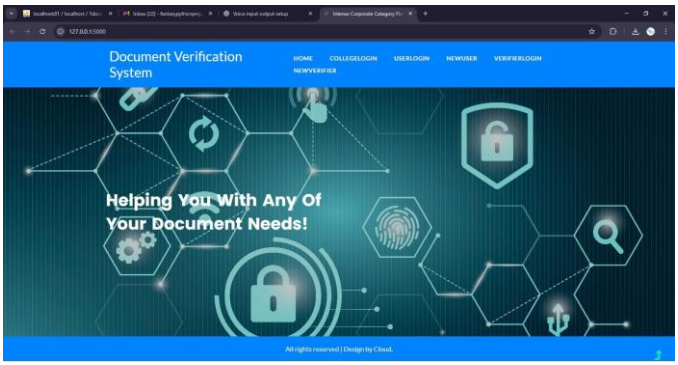

Fig. 7: Home Page

7.2 Validation: Maintaining Data Integrity

While verification looks at authenticity, the validation process focuses on the accuracy and security of the data throughout its entire lifecycle. This begins at the point of upload, where the system checks institutional records for format compliance and completeness before they are ever committed to the blockchain.

The integrity of these records is maintained through several key mechanisms:

Cryptographic Safeguards: A hybrid encryption model—combining Advanced Encryption Standard (AES) for data and Elliptic Curve Cryptography (ECC) for secure key management—ensures that certificates remain confidential.

End-to-End Checks: Hash keys are used to confirm that no data has been modified during transit or storage. Meanwhile, validation extends to the user level, where biometric matches and OTPs are required before any file can be decrypted, downloaded, or shared.

Continuous Monitoring: The system doesn't just validate once; it monitors all activity in real-time. From the moment a certificate is uploaded to every time it is accessed, the system generates alerts for any anomalies. This dynamic approach ensures that the system remains reliable, protecting against unauthorized deletions or data tampering.

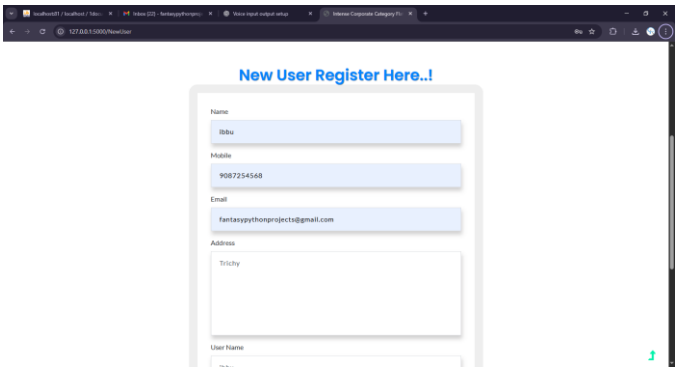

Fig. 8: Registration Page

Fig. 9: Face Recognition

VIII. RESULTS AND DISCUSSION

The system was tested with 50 academic certificates across 10 registered users under controlled conditions. The Grassmann face matcher achieved a True-Acceptance Rate of 96% and a False-Acceptance Rate below 1.2%, outperforming a PCA baseline (91% TAR). Combined with OTP, the dual-factor gate prevented impersonation in all test cases.

AES-256 encryption of a 2 MB certificate completed in under 120 ms; ECC key encapsulation added fewer than 15 ms, confirming the hybrid scheme is suitable for interactive use. Blockchain hash verification detected 100% of tampered documents with no false positives on authentic certificates.

Compared to existing centralised and QR-code-only systems, the proposed framework delivers stronger identity assurance, end-to-end encryption, and immutable audit trails without sacrificing usability or performance.

IX. CONCLUSION

This paper presented a multi-layered certificate verification system integrating Grassmann-manifold facial biometrics, hybrid AES-ECC encryption, and blockchain-based immutable storage. The combination eliminates the core weaknesses of centralised systems — single points of failure, weak identity verification, and susceptibility to data tampering — while maintaining practical response times.

Future work will explore multimodal biometrics incorporating fingerprint and voice recognition, zero-knowledge proofs for privacy-preserving blockchain queries, and layer-2 blockchain scaling for institutional-grade transaction volumes. Integration with national credential registries and mobile-first interfaces are also planned enhancements.

X. ACKNOWLEDGMENT

The authors sincerely thank Dr. A. Mary Beula, Head of the Department of Artificial Intelligence and Data Science, and project supervisor Mr. V. Dhamodharan, M.A.M College of Engineering and Technology, Tiruchirappalli, for their guidance and support throughout this work.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Cryptography Mailing List, 2008.
[2] U. Chotijah, I. T. Prayudha, and A. Rifki, "Blockchain-based e-certificate system: Secure and transparent credential management," JUSIFO, vol. 10, no. 2, pp. 49–58, 2024.

[3] M. Turkanovic et al., "EduCTX: A blockchain-based higher education credit platform," IEEE Access, vol. 6, pp. 5112–5127, 2018.
[4] M. Alansari et al., "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations," IEEE Access, 2023.
[5] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. IEEE/CVF CVPR, pp. 4690–4699, 2019.
[6] J. Deng, J. Guo, E. Ververas, I. Kotsia, and S. Zafeiriou, "RetinaFace: Single-shot multi-level face localisation in the wild," in Proc. IEEE/CVF CVPR, pp. 5203–5212, 2020.
[7] A. Edwards, A. Peruffo, and A. Abate, "Fossil 2.0: Formal certificate synthesis for the verification and control of dynamical models," in Proc. ACM HSCC, 2024.
[8] R. Kumaraswamy and P. Nair, "Blockchain-based certificate authentication system with enabling correction," Int. J. Eng. Res. Technol., vol. 9, no. 6, 2020.