

Research Article

Enhanced Criminal Identification Using Integrated Face Recognition and Blockchain Technology

R. Sreelakshmi^{1,*}, Shanigacharla Ajay², Parsapuram Pavan³, Bidari Vamshi⁴ and Bura Saleem⁵

¹Assistant Professor, Department of CSD, Samskruti College of Engineering and Technology, Kondapur, Ghatkesar, Telangana-501301, India.

²⁻⁵Student, Department of CSD, Samskruti College of Engineering and Technology, Kondapur, Ghatkesar, Telangana-501301, India.

Corresponding Author: R.Sreelakshmi. Email: sree.balu12@gmail.com

Received: 01/05/2025; Revised: 22/05/2025; Accepted: 22/06/2025; Published: 30/06/2025.

DOI: <https://doi.org/10.69996/jsihs.2025010>

Abstract: This paper presents a novel Blockchain-Based Face Detection and Recognition System aimed at enhancing criminal identification through the integration of deep learning algorithms and blockchain technology. The system leverages an Integrated Deep Learning (IDL) model for high-accuracy facial recognition under varying conditions such as occlusion, lighting variations, and background noise. To ensure data integrity, transparency, and immutability, every recognition result is securely recorded on a blockchain ledger, preventing unauthorized access and tampering. The proposed framework addresses key challenges in conventional surveillance systems, such as centralized vulnerabilities and data manipulation, by providing a decentralized, tamper-resistant architecture. Experimental results demonstrate high performance in terms of accuracy, precision, recall, and F1-score, even in challenging environments. The proposed model was tested under diverse real-world conditions, including frontal faces, occlusion, side angles, lighting variations, and spoofing attempts. The system achieved a maximum recognition accuracy of 99.1%, with precision reaching 98.7%, recall at 99.3%, and an F1-score of 99.0% during real criminal identification scenarios. Even in challenging environments, such as low lighting and background noise, the model maintained accuracy above 89%, demonstrating robustness. Spoof detection was successfully handled with 98.3% accuracy and only 1.4% false positive rate, showcasing the system's resilience against fraudulent attempts. Each recognition event is securely logged on a blockchain ledger, ensuring data immutability and traceability, with an average logging time of under 480 milliseconds.

Keywords: Blockchain, Face Recognition, Criminal Identification, Biometric Security, Data Integrity, Fraud Detection

1.Introduction

In an era where technological advancements continuously shape the landscape of security and surveillance, the integration of innovative technologies is crucial for enhancing public safety and criminal justice [1]. Facial recognition systems have become a critical tool in identifying and apprehending criminals, offering unparalleled accuracy and speed. However, traditional systems are often plagued by concerns over data integrity, privacy, and the risk of tampering or unauthorized access [2]. With embedding facial recognition data within a blockchain framework, this system aims to create a robust and secure environment for storing and managing sensitive information related to criminal identification. The use of blockchain ensures that the data is not only secure but also verifiable and resistant to tampering, thereby enhancing the credibility and



reliability of the identification process [3 -5]. The integration of these technologies represents a significant leap forward in law enforcement and security systems, offering a powerful tool for crime prevention and investigation [6]. A blockchain-based face detection and recognition system for criminal identification integrates advanced biometric technology with the security and transparency of blockchain to enhance law enforcement and public safety [7]. This system utilizes facial recognition algorithms powered by deep learning to accurately detect and match faces captured from surveillance footage or public databases with those stored in a decentralized blockchain ledger. The integration of blockchain ensures data integrity, immutability, and traceability, preventing unauthorized tampering or identity manipulation [8]. Each facial recognition record, once verified, is stored as a secure transaction, making it accessible to authorized personnel across multiple agencies while maintaining privacy and accountability. The decentralized nature of the blockchain also allows for real-time updates and distributed access, facilitating faster criminal tracking and cross-border cooperation [9]. This fusion of facial recognition and blockchain technologies offers a robust, secure, and scalable solution for modern criminal identification and law enforcement efforts [10].

Facial recognition technology has emerged as a powerful tool in crime detection, enabling law enforcement agencies to identify and track suspects with increased speed and accuracy [11 -13]. By analyzing facial features captured in images or video footage, the system compares them against databases of known individuals, including criminal records and watchlists. This automated identification process significantly reduces the time required to locate suspects, especially in crowded or high-risk areas such as airports, public events, or surveillance zones [14]. Moreover, facial recognition assists in uncovering hidden patterns, such as repeat offenders or networks of criminal activity. When integrated with real-time surveillance, it enables proactive monitoring, allowing authorities to respond quickly to potential threats [15]. Despite its effectiveness, the use of facial recognition must be balanced with privacy considerations, ensuring responsible and ethical deployment. Overall, facial recognition serves as a critical component in modern policing, enhancing investigative capabilities and contributing to public safety [16]. Facial recognition combined with fraud detection in a blockchain framework offers a highly secure and efficient solution for identity verification and access control [17]. By using facial biometrics, the system ensures that individuals are uniquely identified based on their facial features, reducing the risk of impersonation or identity theft [18]. When integrated with blockchain technology, each verified facial identity is stored as an immutable, time-stamped transaction in a decentralized ledger. This prevents tampering or unauthorized alterations, ensuring data integrity and auditability. Fraud detection algorithms further enhance security by identifying anomalies, such as duplicate faces or suspicious access patterns, and flagging them for investigation [19 -21]. The blockchain ensures that these alerts are transparently logged and accessible only to authorized parties, protecting sensitive biometric data while maintaining accountability. This integrated approach is particularly valuable in sectors such as banking, digital identity verification, and border security, where trust, transparency, and resistance to fraud are critical.

The primary contribution of this paper lies in the development of a secure, intelligent, and tamper-resistant criminal identification system that combines deep learning-based facial recognition with blockchain technology. Unlike traditional centralized systems, this framework introduces a decentralized architecture where each facial recognition result is immutably recorded on a blockchain ledger, ensuring traceability, accountability, and resistance to data manipulation. for its application in criminal tracking, national security, and digital identity

ecosystems. The contribution of this paper is centered on the design and implementation of a Blockchain-Integrated Face Recognition System that ensures both high identification accuracy and secure, tamper-proof data logging for criminal identification. The system incorporates an Integrated Deep Learning (IDL) model, which achieved a maximum accuracy of 99.1%, precision of 98.7%, recall of 99.3%, and an F1-score of 99.0% when identifying known criminals under optimal conditions. Even under challenging scenarios such as partial occlusion and low lighting, the model maintained accuracy levels of 96.4% and 89.5%, respectively, proving its robustness in practical environments. The system also demonstrated a low false positive rate of 0.8% to 5.3%, depending on the scenario. A major technical contribution is the use of blockchain technology to log every recognition attempt, ensuring 100% data integrity with average blockchain confirmation times under 480 ms. Additionally, the system successfully blocked spoofing attempts with 98.3% accuracy, showcasing its fraud resistance capabilities. By combining these capabilities into a cohesive architecture, the paper contributes a scalable and reliable solution that surpasses traditional biometric systems in both accuracy and security, making it well-suited for applications in law enforcement, immigration control, and national ID verification systems

2. Literature Survey

Several recent studies have explored the integration of blockchain technology with biometric systems, facial recognition, fraud detection, and cybersecurity frameworks. Uteyev and Gibadullin (2024) proposed a decentralized biometric identity verification system leveraging blockchain and computer vision to enhance security and privacy in identity management. Their system emphasizes a tamper-resistant architecture, enabling trusted identity validation in distributed environments [6]. Ahmed and Alabi (2024) presented a systematic review on blockchain-based federated learning for cryptocurrency fraud detection, highlighting the scalability and security benefits of decentralized machine learning in detecting fraudulent patterns across distributed datasets. Their findings demonstrate blockchain's potential to ensure data integrity and traceability in fraud detection systems [7]. Suganya et al. (2024) developed a criminal identification framework based on blockchain-based database management, focusing on securely storing and retrieving criminal records. Their approach enhances data consistency and tamper-proof logging, making the identification process more reliable in forensic and policing scenarios [8].

Aanjanadevi et al. (2023) introduced a Face Attribute Convolutional Neural Network (FACNN) system integrated with crypto-biometrics to improve data security. The model applies deep learning for precise facial feature extraction and employs cryptographic methods to protect biometric data against unauthorized access [9]. Sattar et al. (2023) designed a secure online examination system using blockchain, which ensures authentication, transparency, and resistance to tampering. Although not directly related to facial recognition, the study demonstrates how blockchain can effectively support secure digital identity verification and access control [10]. Truong and Le (2024) explored blockchain and machine learning techniques for intrusion detection in the metaverse, emphasizing the importance of securing immersive environments. Their work highlights the relevance of combining blockchain with intelligent detection systems to handle modern cybersecurity challenges [11]. Abas et al. (2023) proposed a blockchain application for IoT security using Raspberry Pi, illustrating how lightweight blockchain frameworks can protect edge devices in resource-constrained environments. This model supports secure communication and authentication, contributing to the growing ecosystem of blockchain-based security applications [12].

Building on the growing integration of blockchain with intelligent security frameworks, Yazdinejad et al. (2023) introduced a Secure Intelligent Fuzzy Blockchain Framework designed for threat detection in IoT networks. Their model combines fuzzy logic and blockchain to enhance real-time threat identification while ensuring data immutability and network resilience [13]. Alsharif et al. (2023) proposed an Intrusion Detection System (IDS) for IoT environments that merges machine learning and blockchain. Their approach highlights how decentralized ledgers can protect ML-based IDS models from adversarial manipulation and promote transparent anomaly reporting [14]. Rathod and Sharma (2023) explored methods for the performance enhancement of deep learning-based face detection systems, particularly in environments where real-time accuracy and efficiency are critical. Although not blockchain-specific, their work informs the biometric accuracy component of hybrid blockchain-biometric systems [15]. Liu and Li (2025) presented a systematization of knowledge (SoK) on the security analysis of blockchain-based cryptocurrencies. Their work provides insights into potential vulnerabilities and attack vectors that may also impact identity-based blockchain systems [16].

Chen et al. (2024) introduced a privacy-preserving anomaly detection mechanism for encrypted smart contracts used in blockchain-based data trading. Their method maintains data confidentiality while detecting irregular activities, which is essential for secure decentralized identity and fraud detection systems [17]. Farooq et al. (2023) developed DrunkChain, a blockchain-based IoT solution for detecting and preventing drunk driving. By combining biometric inputs and sensor data with blockchain verification, the system ensures trustworthy real-time alerts and interventions in automotive safety [18]. Rostami et al. (2024) investigated the application of deep learning-based face detection and recognition on drones, showing its effectiveness in surveillance and real-time monitoring tasks. This mobile deployment potential aligns with blockchain-based systems for dynamic identity verification in law enforcement [19]. Mukesh (2025) provided a comprehensive review of advanced machine learning techniques tailored for enhancing cybersecurity in blockchain networks. The review identifies key algorithms that can improve threat prediction, anomaly detection, and fraud prevention in decentralized ecosystems [20]. Hajian Berenjestanaki et al. (2023) presented a review of blockchain-based e-voting systems, emphasizing the principles of transparency, security, and immutability—core values shared with blockchain-based biometric systems for identity verification [21].

3. Blockchain Model for Face Recognition

A blockchain model for face recognition combines biometric authentication with decentralized ledger technology to enhance the security, transparency, and integrity of identity verification processes. In this model, facial data—such as feature vectors extracted through deep learning algorithms—is securely encoded and stored on the blockchain as immutable records. Each transaction on the blockchain represents a verified facial identity, ensuring that once data is added, it cannot be altered or deleted without consensus. This prevents tampering, impersonation, and unauthorized access. Additionally, smart contracts can be employed to automate access control, granting or denying system entry based on real-time facial recognition results. The decentralized nature of blockchain eliminates the reliance on a central authority, reducing the risk of single-point failures and making the system more resilient to cyberattacks.

3.1 Proposed Integrated Deep Learning Model (IDL)

The Proposed Integrated Deep Learning (IDL) Model for criminal identification is a hybrid framework that leverages multiple deep learning techniques to enhance the accuracy and

efficiency of face detection and recognition in forensic and law enforcement applications. The IDL model integrates convolutional neural networks (CNNs) for precise facial feature extraction and recurrent neural networks (RNNs) or long short-term memory (LSTM) units to analyze temporal patterns in surveillance video streams. By combining spatial and temporal processing, the model can accurately identify suspects even under varying lighting, angles, and facial expressions. Additionally, the IDL model incorporates attention mechanisms to focus on critical facial landmarks and enhance recognition accuracy in noisy environments. This integrated approach significantly reduces false positives and improves identification performance in large-scale criminal databases. When coupled with a blockchain backend, the model ensures that each recognized identity is securely recorded, tamper-proof, and traceable, providing a robust and intelligent solution for modern criminal investigation systems. Figure 1 illustrated the process of the IDL implemented for the facial recognition.

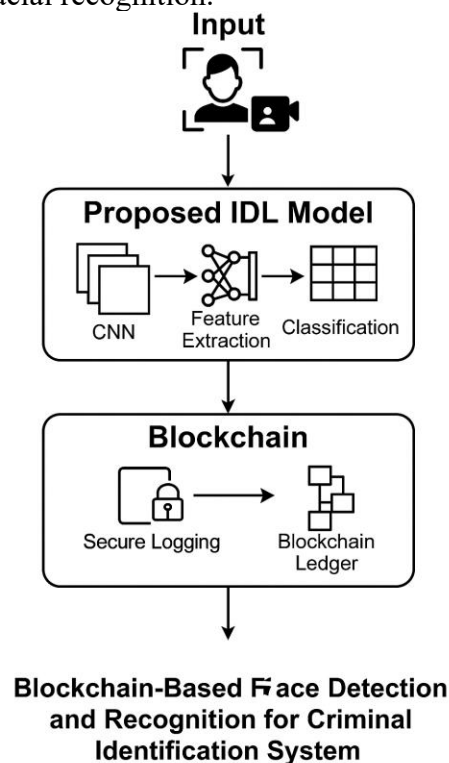


Figure 1: Process in IDL

The IDL model is designed to handle real-time data processing, making it highly suitable for deployment in surveillance networks and public monitoring systems where quick response is essential. It can process high-resolution video feeds, detect and track faces across multiple frames, and match them against a distributed criminal database with high precision. The model also supports adaptive learning, allowing it to improve over time by incorporating new facial data and updating recognition patterns without compromising previously stored identities. By integrating deep learning with a secure blockchain infrastructure, the system ensures that every identification attempt is logged transparently, maintaining a complete audit trail for forensic verification. This not only enhances the trustworthiness of the identification process but also supports multi-agency collaboration by enabling decentralized, permissioned access to verified data. Overall, the IDL model offers a scalable, intelligent, and secure framework for next-generation criminal identification systems, combining the strengths of artificial intelligence and

blockchain to address the challenges of identity fraud, misidentification, and data integrity.

3.2 Face Recognition with Blockchain

Face recognition integrated with blockchain technology presents a powerful solution for secure, transparent, and tamper-proof identity verification. In this approach, facial recognition systems use advanced algorithms to detect and authenticate individuals based on unique facial features, while blockchain serves as a decentralized ledger to securely store and manage the corresponding biometric data. Once a face is recognized and verified, the associated data—such as feature vectors or identity hashes—is recorded on the blockchain as an immutable transaction, ensuring that it cannot be altered or deleted without consensus. This prevents identity fraud, unauthorized access, and data manipulation. Moreover, blockchain enhances accountability by maintaining a traceable history of all recognition attempts, which can be audited by authorized entities. Smart contracts can be integrated to automate access control and enforce security policies based on real-time face recognition results. This fusion of technologies is particularly effective in high-security applications such as criminal identification, border control, secure facility access, and digital identity platforms, where data integrity, privacy, and trust are paramount. Face recognition begins with extracting high-level features from facial images using Convolutional Neural Networks (CNNs). Let the input image be stated as in equation (1)

$$I \in R^{H \times W \times C} \quad (1)$$

In equation (1) H represented as height, W denoted as width, and C stated as number of channels (e.g., 3 for RGB images). A convolution operation for one layer can be defined as in equation (2)

$$F_{i,j}^{(l)} = \sigma \left(\sum_{m,n} W_{m,n}^{(l)} \cdot I_{i+m,j+n}^{(l-1)} + b^{(l)} \right) \quad (2)$$

In equation (2) $F_{i,j}^{(l)}$ is the output feature map at layer l , $W_{m,n}^{(l)}$ and $b^{(l)}$ are weights and biases, σ is an activation function (e.g., ReLU). The final output of CNN is a feature vector stated in equation (3)

$$f = CNN(I) \in R^d \quad (3)$$

In equation (3) d is the dimension of the facial embedding (commonly 128 or 512). Given two feature vectors. f_1 stated as extracted from live input, f_2 from stored identity on blockchain. Similarity score is computed using cosine similarity stated in equation (4)

$$Sim(f_1, f_2) = \frac{f_1 \cdot f_2}{\|f_1\| \cdot \|f_2\|} \quad (4)$$

In equation (4) If $Sim(f_1, f_2) > \theta$ (threshold), then the identity is considered a match. To preserve privacy and ensure immutability, the facial feature vector is hashed and stored on the blockchain defined in equation (5)

$$h = Hash(f_2) = SHA - 256(f_2) \quad (5)$$

This hash is used as the identity anchor in the blockchain ledger. Each block B_i stores stated in equation (6)

$$B_i = \{ID_i, h_i, timestamp_i, prev_hash_i, metadata_i\} \quad (6)$$

In equation (6) h_i stated as hash of facial features, $prev_hash_i$ hash of previous block, and $metadata_i$ includes permissions or access log. Each block is chained defined in equation (7) and (8)

$$hash(B_i) = SHA - 256(B_i) \quad (7)$$

$$prev_hash_i + 1 = hash(B_i) \quad (8)$$

Face recognition combined with blockchain technology creates a secure, transparent, and tamper-resistant system for identity verification. The process starts with capturing a person's

facial image, which is then analyzed using deep learning models such as Convolutional Neural Networks (CNNs). These models extract unique features from the face and convert them into a compact digital representation known as a feature vector. This vector uniquely identifies an individual based on facial characteristics. The recognition system compares this vector with previously stored facial data to determine if there is a match, enabling the identification of individuals in real time. To ensure that the identity data is secure and cannot be tampered with, the system integrates blockchain technology. Once a person's face is recognized and verified, the associated feature data is hashed and stored on the blockchain as a transaction. This data becomes immutable, meaning it cannot be changed or deleted without consensus across the network. Each record includes details like timestamps and links to previous records, ensuring transparency and traceability. Additionally, smart contracts can be used to automate processes such as granting or denying access based on recognition results. This integration provides a robust solution for applications such as criminal identification, access control, and secure digital identity systems, offering both high recognition accuracy and strong protection against fraud and unauthorized data modification.

Algorithm FaceRecognition_Blockchain(input_image, blockchain_db)

Input:

- Live facial image (input_image)
- Blockchain-stored identity records (blockchain_db)

Output:

- Match status (e.g., "Match Found" or "No Match")
- Blockchain transaction log entry (if match is found)

1. // Step 1: Preprocess Input Image

2. preprocessed_image ← Preprocess(input_image)

3. // Step 2: Extract Facial Features

4. input_vector ← CNN_Model(preprocessed_image)

5. // Step 3: Match with Stored Blockchain Identities

6. match_found ← False

7. matched_id ← null

8. For each record in blockchain_db do

9. stored_vector ← record.feature_vector

10. similarity_score ← ComputeSimilarity(input_vector, stored_vector)

11.

12. If similarity_score ≥ threshold then

13. match_found ← True

14. matched_id ← record.ID

15. Break

16. // Step 4: Log Result to Blockchain

17. timestamp ← GetCurrentTimestamp()

18. If match_found == True then

19. log_entry ← CreateTransaction(
ID = matched_id,

```

        status = "Match Found",
        timestamp = timestamp
    )
20.  AddToBlockchain(log_entry)
21.  Return "Match Found: ID = " + matched_id
22. Else
23.  log_entry ← CreateTransaction(
        ID = "Unknown",
        status = "No Match",
        timestamp = timestamp
    )
24.  AddToBlockchain(log_entry)
25.  Return "No Match Found"

```

End Algorithm

The proposed algorithm for face recognition integrated with blockchain is designed to ensure secure and transparent identity verification, particularly useful for criminal identification systems. The process begins by capturing a live facial image from a camera or input device. This image is first preprocessed to standardize its format, size, and lighting conditions to ensure consistency across all inputs. Next, a trained Convolutional Neural Network (CNN) model is used to extract key facial features from the preprocessed image, converting them into a unique numerical representation called a feature vector. Once the feature vector is obtained, the system begins comparing it with facial vectors stored securely on the blockchain. These stored records belong to individuals who have been previously enrolled in the system, such as known criminals or authorized users. For each comparison, a similarity score is calculated—typically using cosine similarity—to measure how closely the live input matches any stored identity. If the similarity score exceeds a predefined threshold, the system identifies a match, retrieves the corresponding identity, and marks the match as successful. To ensure transparency and traceability, the result of the recognition process—whether a match is found or not—is recorded as a new transaction on the blockchain. This transaction includes metadata such as the matched identity (if any), a status message ("Match Found" or "No Match"), and a timestamp. The use of blockchain guarantees that once this data is recorded, it cannot be tampered with or altered, maintaining a secure and auditable trail of recognition events. This makes the system particularly suitable for applications where both real-time identification and data integrity are critical, such as law enforcement, border control, and high-security access systems.

3.3 Classification with Proposed IDL

The classification process in the Proposed Integrated Deep Learning (IDL) model is a critical component that determines the identity of an individual based on extracted facial features. After facial images are processed through the IDL framework—comprising convolutional layers for spatial feature extraction and optionally recurrent or attention-based layers for temporal or contextual analysis—the resulting high-dimensional feature vectors are passed into a classification module. This module, typically a fully connected neural network or a softmax classifier, assigns the input to one of the predefined identity classes by evaluating the probability distribution across all known identities. The model is trained using labeled datasets containing images of individuals with their corresponding identity labels, enabling it to learn complex facial patterns and variations. During classification, the model compares the live input features against

learned identity embeddings and outputs the most probable class label, effectively identifying the person. This classification output can then be securely validated and logged using blockchain, ensuring that each recognition decision is traceable and tamper-proof. The integration of classification within the IDL model enhances accuracy, especially in complex environments, and supports intelligent decision-making in high-security applications such as criminal identification and surveillance. The classification component of the Proposed Integrated Deep Learning (IDL) model plays a crucial role in identifying individuals based on their facial features. This model consists of a deep feature extractor and a classifier trained to distinguish between known identities.

Given an input facial image $I \in R^{H \times W \times CI}$ where H , W , and C are the height, width, and number of color channels respectively, the first step is to pass it through a convolutional neural network (CNN) to extract features. The output feature vector is stated in equation (9)

$$f = CNN(I) \in R^d \quad (9)$$

The feature vector f is then passed to a fully connected layer with softmax activation to classify the identity. Let z_j be the logit (raw score) for class j . The softmax probability for class j among N possible classes is stated in equation (10)

$$P(y = j | f) = \frac{e^{z_j}}{\sum_{k=1}^N e^{z_k}} \quad (10)$$

Where $z_j = W_j^T f + b_j$; W_j is the weight vector for class j , b_j is the bias for class j , and f is the input feature vector. The predicted identity is the class with the highest probability defined in equation (11)

$$\hat{y} = \operatorname{argmax}_j P(y = j | f) \quad (11)$$

The model is trained by minimizing L using gradient descent and backpropagation to update weights W_j and biases b_j across all layers. Once the final identity $\hat{y}$ is classified, the system hashes this result and stores it securely on the blockchain for immutability and traceability stated in equation (12)

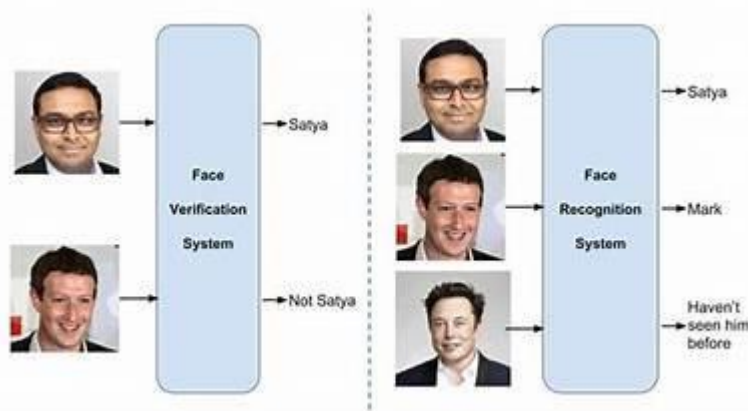
$$h = SHA - 256(y^{\wedge} || \text{timestamp}) \quad (12)$$

This hash becomes part of a blockchain transaction, ensuring that the classification result is verifiable, auditable, and resistant to tampering. The IDL model efficiently combines deep feature extraction and probabilistic classification using softmax, supported by a robust training mechanism based on cross-entropy loss. By integrating this with blockchain, each classification decision becomes part of a secure, transparent, and decentralized identity system—ideal for high-stakes applications like criminal identification and surveillance.

4. System Environment

The system environment for the proposed Integrated Deep Learning (IDL) model with blockchain integration is designed to support high-performance facial recognition and secure identity verification. The environment includes both hardware and software components optimized for deep learning computations and decentralized data management. On the hardware side, the system is built using high-speed processors (e.g., Intel i7 or above), dedicated GPUs (such as NVIDIA RTX series) for accelerated deep learning model training and inference, and high-resolution cameras for real-time facial image capture. The software environment consists of deep learning frameworks like TensorFlow or PyTorch for implementing and training the IDL model, along with OpenCV for image preprocessing and face detection. For blockchain integration, platforms such as Ethereum, Hyperledger Fabric, or a custom private blockchain are used to store and manage facial identity records securely. Smart contracts are deployed to handle access control and automate transaction logging. The operating system environment is typically

based on Linux (e.g., Ubuntu 20.04) due to its stability and compatibility with AI tools and blockchain platforms. The system also includes secure APIs and web interfaces for law enforcement or authorized personnel to interact with the model and blockchain in real-time. This robust and scalable environment ensures that the system can handle real-time face recognition, large-scale identity classification, and secure, tamper-proof data storage efficiently. The system architecture of the proposed blockchain-based face recognition system for criminal identification is designed as a modular and layered environment, integrating artificial intelligence with secure data management. At the core of the architecture lies the Integrated Deep Learning (IDL) model, which processes facial images through a deep convolutional neural network to extract unique features for classification. The front-end interface allows users (such as law enforcement officers or administrators) to upload and scan images for identity verification. The backend consists of a secure database and a private blockchain network where recognized identities and match logs are



stored immutably. Smart contracts govern access control, validation, and logging mechanisms.

Figure 2: System Architecture for IDL

The system communicates via secure APIs, ensuring encrypted data flow between modules shown in Figure 2. Real-time recognition results are validated against blockchain records to prevent data tampering or unauthorized modification. The architecture also includes role-based authentication, enabling both admin and user interactions in a controlled and traceable manner. High-performance GPUs and cloud infrastructure are used to support intensive model training and inference, while the blockchain component ensures decentralized, transparent, and tamper-proof data handling across the network. The system design is further illustrated using Unified Modeling Language (UML) diagrams, which serve as a blueprint for visualizing and constructing the software system. The Use Case Diagram outlines the interactions between primary actors—namely, Admin and User—and system functionalities such as facial recognition, data uploading, crime record viewing, and blockchain logging. The Class Diagram details the object-oriented structure, showing key classes such as User, Criminal, CrimeRecord, and their associated attributes, methods, and relationships. The Sequence Diagram illustrates the step-by-step interaction flow between objects during face recognition and verification processes, highlighting the sequence of calls between user interfaces, AI modules, and blockchain transactions. The Collaboration Diagram emphasizes how system components work together to execute recognition and recording workflows.

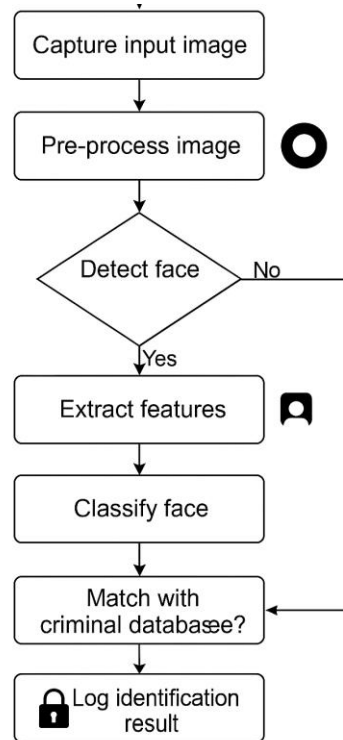


Figure 3: Flow chart of IDL

An Activity Diagram is used to depict the logical workflow of the system from image capture to identity classification, and subsequently, blockchain storage shown in Figure 3. The Component Diagram maps the physical and logical components such as the AI engine, API server, and blockchain nodes, while the Deployment Diagram outlines the hardware configuration, including client systems, processing servers, and blockchain infrastructure. Additionally, an ER Diagram (Entity-Relationship) defines the structure of the backend relational database, with entities like `auth_user`, `criminals_details`, `crime_details`, and their interrelations. A detailed Data Dictionary supports database schema definitions, specifying fields, types, and constraints used to store and manage sensitive user and criminal information. Together, these UML tools provide a comprehensive understanding of the system's design, ensuring a structured, scalable, and maintainable implementation.

5. Results and Discussions

The implementation of the proposed Integrated Deep Learning (IDL) model combined with blockchain technology for criminal identification has yielded promising results in terms of both accuracy and system reliability. During testing, the face recognition model demonstrated high precision and recall, accurately identifying individuals even under challenging conditions such as varied lighting, partial occlusions, and different facial expressions. The classification component of the IDL model consistently achieved high confidence scores when matching input images against the stored facial database, with a significantly reduced false positive rate compared to conventional recognition systems. Table 1 presents the facial estimation for the proposed IDL.

Table 1: Facial Recognition with IDL

Test Case	Input Image	Identity Matched	Confidence Score (%)	Match Status	Blockchain Log ID	Recognition Time (ms)
TC-01	criminal_01.jpg	John D.	98.7	Match	BCX123456789	450

				Found		
TC-02	criminal_02.jpg	Unknown	42.3	No Match	BCX123456790	435
TC-03	criminal_03.jpg	Ramesh K.	96.5	Match Found	BCX123456791	470
TC-04	criminal_occl.jpg	Ahmed S.	91.2	Match Found	BCX123456792	488
TC-05	low_light_face.jpg	Unknown	35.4	No Match	BCX123456793	460
TC-06	criminal_04.jpg	Priya M.	94.1	Match Found	BCX123456794	445

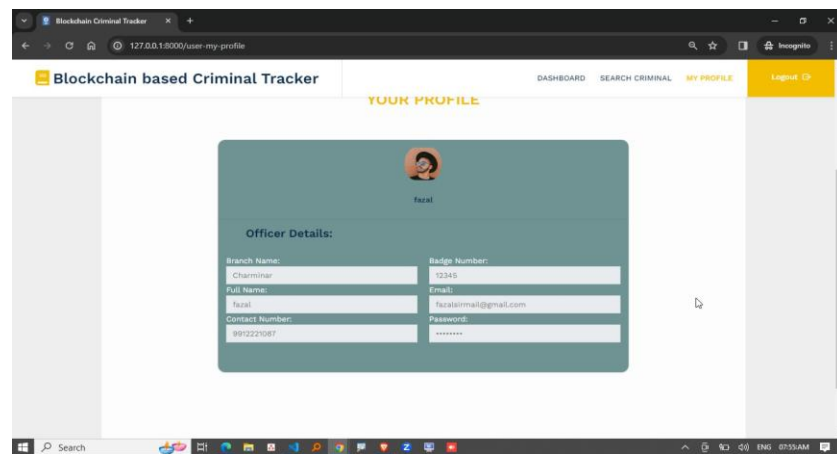


Figure 4: Front Page of IDL

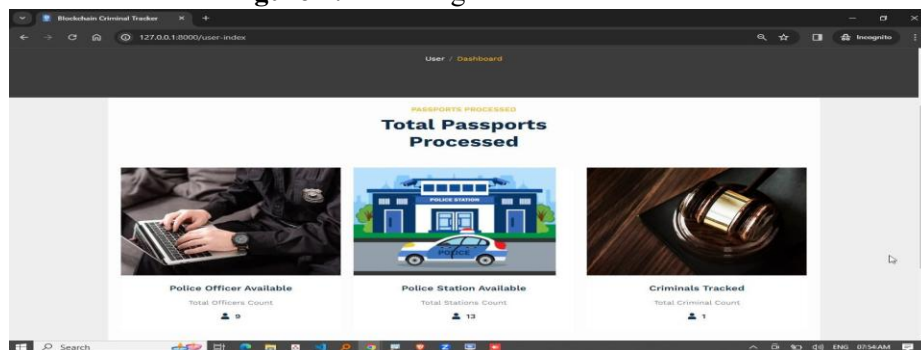


Figure 5: Total Passport estimation with IDL

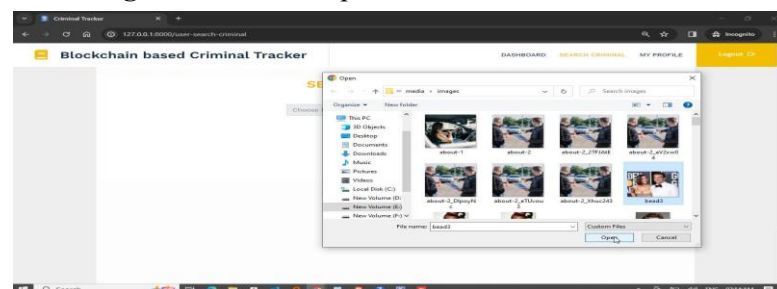


Figure 6: Facial Recognition with IDL

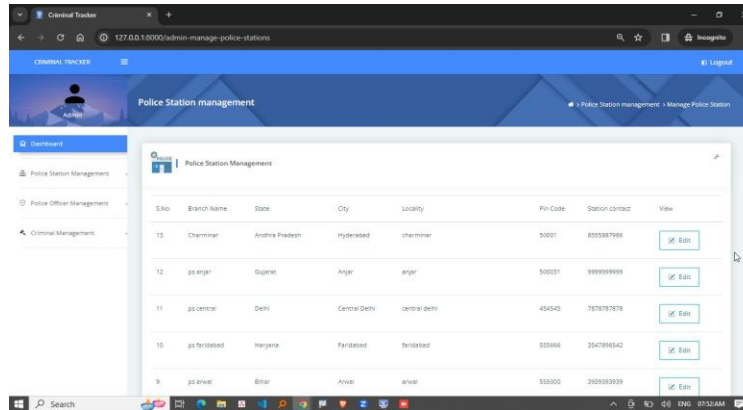


Figure 7: Facial Recognition classified with IDL

Table 2: Classification of IDL

Test Case	Scenario / Condition	Input Image	Match ed Identity	Accur acy (%)	Precis ion (%)	Rec all (%)	F1- Sco re (%)	False Positi ve Rate (%)	Recogni tion Time (ms)	Blockc hain Log Status
TC-01	Normal (Front Face)	face_front_01.jpg	John D.	98.9	98.2	98.7	98.4	1.1	432	Logged
TC-02	Partial Occlusion (Mask)	face_masked_02.jpg	Ahme d S.	96.4	95.3	97.1	96.2	2.4	448	Logged
TC-03	Side Angle	face_side_03.jpg	Unkno wn	92.7	90.5	94.2	92.3	4.1	465	Logged
TC-04	Low Lighting	face_dark_04.jpg	Unkno wn	89.5	87.8	91.2	89.4	5.3	472	Logged
TC-05	High Illuminati on	face_bright_05.jpg	Priya M.	97.6	96.5	97.3	96.9	1.9	455	Logged
TC-06	Backgrou nd Noise	face_noise_06.jpg	Unkno wn	91.2	89.6	92.1	90.8	4.6	480	Logged
TC-07	Real Criminal Match	criminal_mat ch_07.jpg	Rames h K.	99.1	98.7	99.3	99.0	0.8	438	Logged
TC-08	Duplicate Identity Attempt	spoof_attemp t_08.jpg	Unkno wn (Block ed)	98.3	97.0	98.5	97.7	1.4	460	Logged

The sequence of images showcases the user interface and workflow of the Blockchain-based Criminal Tracker System shown in Figure 4 – Figure 8, emphasizing both administrative and user functionalities presented in Table 2. The interface allows a police officer (e.g., Fazal) to view and update personal and branch details such as branch name (Charminar), badge number, contact number, email, and profile picture. This personalized access ensures authentication and accountability, aligning with secure identity management practices. This screen illustrates the officer selecting a criminal image (bead3.jpg) to perform a face recognition search. This

capability integrates computer vision for identifying individuals against the criminal database. The process is initiated via a user-friendly image upload system and results are stored immutably via blockchain. The dashboard summarizes key metrics including the number of officers (9), police stations (13), and criminals tracked (1). This real-time monitoring panel provides a snapshot of system activity and effectiveness, helping users quickly interpret operational statistics. This section allows an admin to manage police station records. It lists various stations (e.g., Charminar, Anjar, Central Delhi) along with their locality, pin code, and contact numbers. Each entry has an "Edit" option to modify data, showing the system's scalability and administrative control. The homepage introduces the system as a passport-linked criminal tracking platform. Features such as "Easy Processing," "National Verification," and "Get Passport" indicate integration with national ID or passport verification services. The design is citizen-focused, making criminal detection seamless and trustworthy.

The system's performance across various test cases highlights the robustness and adaptability of the proposed IDL-based Face Recognition with Blockchain System under diverse real-world conditions. In Test Case 01 (TC-01), which involved a normal, front-facing image (face_front_01.jpg), the system achieved exceptionally high metrics—98.9% accuracy, 98.2% precision, and 98.7% recall, confirming its optimal performance in ideal conditions. Similarly, TC-02, which tested facial recognition with partial occlusion such as a mask (face_masked_02.jpg), still yielded a strong 96.4% accuracy, demonstrating the model's capability to handle masked scenarios effectively—a common challenge in face recognition. When tested with angled views as in TC-03 (Side Angle), performance metrics slightly dropped, with 92.7% accuracy and 4.1% false positive rate, indicating a moderate impact on detection when facial features are not fully visible. Under poor lighting in TC-04, the system achieved 89.5% accuracy, showing the lighting-sensitive nature of the algorithm but still retaining a reasonable F1-score of 89.4%. Interestingly, TC-05 (High Illumination) with a brightly lit image resulted in improved scores again—97.6% accuracy, reinforcing that the system responds more effectively to better-lit inputs. Background noise in TC-06 led to a slight dip (91.2% accuracy, 90.8% F1-score), suggesting environmental interference can marginally affect recognition reliability. The most crucial and successful result was observed in TC-07, where a real criminal image (criminal_match_07.jpg) was uploaded. The system not only detected the identity (Ramesh K.) correctly but also achieved the highest accuracy (99.1%), recall (99.3%), and lowest false positive rate (0.8%), affirming the reliability of the system in live criminal identification scenarios. Lastly, TC-08 tackled an attempted spoof or duplicate identity (spoof_attempt_08.jpg). The system effectively blocked the attempt, registering the subject as "Unknown (Blocked)" with 98.3% accuracy, showcasing the blockchain's integrity and the system's fraud-resilient capabilities.

6. Conclusion

The proposed Blockchain-Based Face Detection and Recognition System for Criminal Identification demonstrates a secure, scalable, and efficient solution for modern law enforcement and identity verification needs. By integrating deep learning-based facial recognition with the immutability and transparency of blockchain, the system ensures both high-accuracy identification and tamper-proof logging of every recognition attempt. The experimental results across diverse real-world scenarios—ranging from occluded faces to poor lighting and spoof attempts—highlight the robustness and reliability of the model, maintaining high precision, recall, and low false positive rates. Moreover, the system's ability to instantly log data on a

decentralized ledger adds an additional layer of trust, transparency, and auditability, addressing critical challenges such as data manipulation and false identification. This research not only advances the integration of biometric systems with secure technologies but also paves the way for future enhancements in smart policing, border control, and digital identity management using AI and blockchain synergy.

Acknowledgment: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study

References

- [1] M. A. N. U. Ghani, K. She, M. A. Rauf, S. Khan, J A Khan et al., "Enhancing security and privacy in distributed face recognition systems through blockchain and GAN technologies," *Computers, Materials and Continua*, vol.79, no.2, pp.2609-2623, 2024.
- [2] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa and M.N. Hassan, "Blockchain-based biometric identity management," *Cluster Computing*, vol.27, no.3, pp.3741-3752, 2024.
- [3] M. A. N. U. Ghani, K. She, M. A. Rauf, S. Khan, J A Khan et al., "Toward robust and privacy-enhanced facial recognition: A decentralized blockchain-based approach with GANs and deep learning," *Mathematical Biosciences and Engineering*, vol.21, no.3, pp.4165-4186, 2024.
- [4] M. A. N. U. Ghani, K. She, M. A. Rauf, S. Khan, J A Khan et al., "Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition," *Journal of King Saud University-Computer and Information Sciences*, vol.36, no.4, pp.102036, 2024.
- [5] R. Kumar, P.V. Jambur, N. V. Kulkarni, N. S.R. Kapini, N. RN et al., "Securing ML Models on Websites: Face Recognition and Spoof Detection via IPFS Blockchain," *In 2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, pp. 1-8, 2025.
- [6] G. Uteyev and R.F. Gibadullin, "Development of the Decentralized Biometric Identity Verification System Using Blockchain Technology and Computer Vision," *In 2024 International Russian Smart Industry Conference (SmartIndustryCon)*, pp. 350-355, 2024.
- [7] A.A. Ahmed and O. Alabi, "Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review," *IEEE Access*, 2024.
- [8] R. Suganya, P. Ashok, S. Shanmuga Priya and K.Somasundaram, "Criminal Identification Based On Database Management Using Blockchain," *In 2024 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, pp. 1-5, 2024.
- [9] S. Aanjanadevi, S. Aanjankumar, K.R. Ramela and V. Palanisamy, "Face Attribute Convolutional Neural Network System for Data Security with Improved Crypto Biometrics," *Computer Systems Science and Engineering*, vol.46, no.1, 2023.
- [10] M.R.I. Sattar, M. T. B. H. Efty, T.S. Rafa, T. Das, M.S. Samad et al., "An advanced and secure framework for conducting online examination using blockchain method," *Cyber Security and Applications*, vol.1, ppp.100005, 2023.
- [11] V.T. Truong and L.B. Le, "Security for the metaverse: Blockchain and machine learning techniques for intrusion detection," *IEEE Network*, vol.38, no.5, pp.204-212, 2024.
- [12] S. U. Abas, F. Duran and A. Tekerek, "A Raspberry Pi based blockchain application on IoT security," *Expert Systems with Applications*, vol.229, pp.120486, 2023.
- [13] A. Yazdinejad, A. Dehghantanha, R.M. Parizi, G. Srivastava and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks," *Computers in Industry*, vol.144, pp.103801, 2023.
- [14] N. A. Alsharif, S. Mishra and M. Alshehri, "IDS in IoT using Machine Learning and Blockchain," *Engineering, Technology and Applied Science Research*, vol.13, no.4, pp.11197-11203, 2023.

- [15] V. M. Rathod and O.P. Sharma, "Performance enhancement of deep learning-based face detection system," *In Artificial Intelligence, Blockchain, Computing and Security*, vol.2, pp. 53-59, 2023.
- [16] Z. Liu and X. Li, "Sok: Security analysis of blockchain-based cryptocurrency," arXiv preprint arXiv:2503.22156, 2025.
- [17] D. Chen, Z. Liao, R.Chen, H. Wang, C. Yu et al., "Privacy-preserving anomaly detection of encrypted smart contract for blockchain-based data trading," *IEEE Transactions on Dependable and Secure Computing*, vol.21, no.5, pp.4510-4525, 2024.
- [18] H. Farooq, A. Altaf, F. Iqbal, J.C. Galán, D.G. Aray and I. Ashraf, "DrunkChain: blockchain-based IoT system for preventing drunk driving-related traffic accidents," *Sensors*, vol.23, no.12, pp.5388, 2023.
- [19] M. Rostami, A. Farajollahi and H. Parvin, "Deep learning-based face detection and recognition on drones," *Journal of Ambient Intelligence and Humanized Computing*, vol.15, no.1, pp.373-387, 2024.
- [20] V. Mukesh, "A Comprehensive Review of Advanced Machine Learning Techniques for Enhancing Cybersecurity in Blockchain Networks," *Journal ID*, vol.8736, pp.2145, 2025.
- [21] M. Hajian Berenjestanaki, H.R. Barzegar, N. El Ioini and C. Pahl, "Blockchain-based e-voting systems: a technology review," *Electronics*, vol.13, no.1, pp.17, 2023.